Carnegie Mellon University
Software Engineering Institute

Cyber Mutual Assistance Workshop Report

Jonathon Monken, PJM Interconnection
Fernando Maymi,PhD, Army Cyber Institute
Dan Bennett, PhD, Army Cyber Institute
Dan Huynh, Army Cyber Institute
Blake Rhoades, Army Cyber Institute
Matt Hutchison, Army Cyber Institute
Judy Esquibel, Army Cyber Institute
Bill Lawrence, North American Electric Reliability Corporation
Katie Stewart, Software Engineering Institute

February 2018

SPECIAL REPORT
CMU/SEI-2018-SR-007

CERT Division

http://www.sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

DM17-0256

Table of Contents

Abstract

This report describes a Cyber Mutual Assistance Workshop (CMAW), its significance, and its outcomes. The CMAW was intended to explore the interconnectedness of the North American Power Sector and possible sources of aid, should the sector fall victim to a cyber attack. The objective of the CMAW was to enable better understanding of capabilities, not only in the sector's own cyber security workforce, but in possible mutual support from city, state, and federal government entities, and across other sectors' cyber security communities. The Army Cyber Institute, alongside the Electric Infrastructure Security Council and the Software Engineering Institute's CERT Coordination Center, aimed to explore and evoke national conversation on the possibility of mutual cyber assistance in times of duress and the importance to that endeavor of prior understanding and relationships between concerned parties.

1 Introduction

1.1 Background

In today's environment, the threat of cyber attacks continues to increase at an alarming rate. The Department of Defense (DoD) Critical Infrastructure Protection (CIP) Plan charges the Army with contributing to the protection infrastructure of the United States (U.S.) against cyber attacks. To successfully defend and protect against cyber attack, the Army, in partnership with industry and other stakeholders, must ensure cyber readiness and operational resilience. Operational resilience is defined as an organization's ability to adapt to risk that affects its core operational capabilities [SEI 2017a]. Mitigating risk of cyber attacks requires a comprehensive strategy to counter, and if necessary, withstand disruptive and destructive attacks. Both public and private partners within various sectors must work together to develop intelligence, warning, and operational capabilities to mitigate sophisticated, malicious cyber attacks before they can impact U.S. interest [DoD 2015].

The Army Cyber Institute (ACI) is tasked with providing innovative ideas to the Army, the DoD, and the nation in order to address future cyber-related challenges. One of the challenges the ACI is exploring is to better understand future full-spectrum and Unified Land Operations in dense urban areas, also known as megacities. The goal is to investigate how to defend against mutually supporting cyber and kinetic threats in dense urban environments. Part of that challenge involves the comprehension of protection of critical infrastructure against cyber attacks. The Department of Homeland Security (DHS) defines 16 Critical Infrastructures and Key Resources (CIKR) [DHS 2017c]. One such CIKR is the energy sector. The ACI is exploring the current model of Regional Mutual Assistance Groups (RMAGs).[1] Within RMAGs, the energy sector's framework, these groups provide each other with operational and technical assistance, to meet cyber capability needs during a large-scale cyber event or attack on the energy sector. While RMAGs provide a legal and financial structure for sharing assets between energy companies, they are currently limited to routine assets such as line/bucket trucks, line repair personnel [BLS 2017], and commodity parts such as poles and wires. The Electricity Infrastructure Security (EIS) Council [EIS Council 2017] is currently working with RMAGs to scope the requirements for cyber capabilities during large-scale and cyber events. The requirements are based on industry need for low-density, critical engineering assets. The initial criteria for determining what cyber capabilities are needed include the following:

- defining baseline skillsets
- programming languages and operating system familiarity
- security clearances/background checks
- number of personnel based on type/scale of event
- likely tasks to be executed, Information Technology (IT) vs. Operations Technology (OT) [Harp 2017]
- deployment scenarios including duration of use and transitions

[1] Quoted on Regional Mutual Assistance Groups (RMAGs) Jonathon Monken, Vice President United States Policy, Operations, EIS Council.

In order to identify challenges in defining cyber requirements for RMAGs and to brainstorm possible solutions, the ACI hosted a Cyber Mutual Assistance Workshop (CMAW).[2] The CMAW took place on March 8, 2016 at Cullum Hall, West Point, N.Y. The workshop was considered phase one of ACI research to better understand RMAGs by examining interdependencies within critical infrastructure.

The CMAW aimed to bring practitioners and experts together to collaborate in a holistic approach in examining issues concerning the energy sector. The scope was centered on mutual assistance [EEI 2016] and the exploration of leveraging or sharing cyber capabilities. During a cyber attack, the most likely course of action will involve coordination with federal-level entities, Information Sharing and Analysis Centers, and intelligence fusion center engagement. However, these top-down management or command and control structures and processes are still being defined.

To have adequate time to achieve our goal, we must begin immediately to identify areas of opportunity for joint cyber missions and capabilities with Army Cyber and infrastructure industry companies. The RMAG framework described earlier is well known within the energy sector and is also referred to as mutual assistance. Particular to mutual assistance, opportunities to improve cyber resilience, response, and recovery among New York State energy providers were identified and are currently under discussion. However, one topic that received a great deal of attention is determining the best way to develop an industry model for cyber mutual aid. This report outlines the findings, conclusions, and recommendations from the workshop.

1.2 Workshop Objectives

The workshop provided an opportunity for practitioners and experts from across the public and private sectors to gather and collaborate in a holistic approach to examine the following issues concerning the energy sector:

- defining requirements for cyber capability
- discussing existing legal and operational frameworks
- partnership development
- multi-sector exercise development

1.3 Workshop Participants

The following organizations were represented at the workshop:

- Army Cyber Institute (ACI-CMAW Lead)
- Electricity Infrastructure Security (EIS) Council (CMAW Co-Lead)
- Carnegie Mellon Software Engineering Institute CERT Program (CMU-SEI-CERT CMAW Lead Facilitator)
- Citigroup – Global Cyber Threat Exercise Team (GCTET)
- Commonwealth Edison (ComEd)

[2] Mention of private sector organizations in this paper does not imply endorsement of the EIS Council, CMU-SEI-CERT or any other organization, by the U.S. government.

- Defense Advanced Research Projects Agency (DARPA)
- Edison Electric Institute (EEI)
- Exelon
- Idaho National Laboratories (INL)
- North American Electric Reliability Corporation (NERC)
- NextEra Energy
- Norwich University Applied Research Institute (NUARI)
- PJM Interconnection
- PowerAdvocate
- SimSpace Corporation
- United States Cyber Command (USCYBERCOM) – Cyber National Mission Force (CNMF)

2 Workshop Findings

2.1 Presentations

At the workshop, there was a series of presentations to invite sharing of initial thoughts on mutual assistance.

- Presentation 1: The Army's Stake in Cyber, presented by Fernando Maymi, Army Cyber Institute, Deputy Director
- Presentation 2: Lessons Learned from GridEX III, presented by Bill Lawrence, Associate Director, Stakeholder Engagement Electricity Information Sharing and Analysis Center (E-ISAC) North American Electric Reliability Corporation (NERC)
- Presentation 3: Energy Sector Mutual Assistance**,** presented by Cheryl Maletich, Vice President Distribution System Operations, Commonwealth Edison
- Presentation 4: The CMA Working Group**,** presented by James Fama, Edison Electric Institute
- Presentation 5: Asset Owner Perspective, a discussion presented by Samara Moore, Exelon
- Presentation 6: Use Cases for Cyber Incidents, a discussion presented by Tom O'Brien, Vice President and Chief Information Officer, PJM Interconnection

The facilitated session explored a set of nine research questions. There were three "themes" that were used to categorize responses to each of the research questions:

- Governance Concerns: covers any responses pertaining to legal, policy, governance, authority, and so on.
- Asset/Talent Management/Workforce Development: covers any responses pertaining to security concerns, configuration management, risk management, and human resources management.
- Partnership Gaps: covers any responses suggesting gaps in communication and knowledge of existing frameworks/systems that result from a lack of communication, information sharing, or situational awareness.

The following sub sections provide a summary of discussions that took place in response to each research question. Refer to Appendix C to view correlated responses captured during the CMAW for each research question.

2.2 What Cyber Interdependencies Do We Need to Consider?

We asked the participants to identify possible interdependencies that would require consideration to implement cyber mutual assistance. There was valuable discussion around various scenarios that provided insight into the required interdependencies. For example, in the case that industry provides power to a military installation and the provider comes under a cyber attack, who will lead the response? How will response to an attack be prioritized? Will the military installation be prioritized over private industry needs in a response? Do the same policies apply for federal, state, and local government entities? Another theme discussed was the challenges of communication ca-

pabilities and intelligence operations. Who is in charge of leading intelligence operations to identify threats? Who is in charge of internal and external communications (including public relations) in the event of a cyber attack? If communications go down, what are the workarounds? At a high level, the group also cited legal and regulatory issues that would need addressing. All of these identified concerns are part of the Governance Concerns perspective defined above.

From the Partnership Gaps perspective, the group discussed the cross-sector impacts, potential third-party issues, and relationships with critical suppliers. The group also identified areas of concern around Asset/Talent Management to include personnel/staffing and vendor support and expertise.

2.3 Cyber Exercises and Their Role in Cyber Mutual Assistance

One way to explore possibilities or enable cyber capability within mutual assistance is through cyber-related exercises, particularly the ones that explore multiple sectors. Development of exercise capabilities is among the objectives within the DoD Strategy that is necessary to defend the nation. The following is one of the DoD Strategy objectives particular to the topic of exercises: "Prepare to conduct cyber operations to defend the nation from cyber attacks of significant consequence. Practice emergency procedures through regular exercise at all levels" [DoD 2015]. Workshop participants were queried on the types of cyber exercises in which their organizations participate. Please reference Appendix C — Responses Corresponding to Research Questions — "Which cyber exercises has your organization participated in?" There were 29 responses shared with emphasis placed on the need to leverage exercises to produce meaningful outcomes and to take advantage of an opportunity to experiment.

What is a cyber exercise?

A cyber exercise may run as a stand-alone event on an isolated network or as an activity within a larger training exercise on an operational network. The planning processes are similar, except that the latter requires additional coordination between the exercise planners to ensure the exercise both achieves the cyber objectives and supports the greater exercise objectives through controlled impacts to operational networks. The exercise planning process begins by identification of the objectives and outcomes of the exercise [Kick 2014].

2.3.1 Types of Cyber Exercises

Cyber exercises are typically hindered by being either overly technical or too high level; for example, managers/operators and the technical personnel are typically not in the same room. Successful cybersecurity training within organizations requires a way that enables creativity and allows for experimentation while conducting organizational collective training. The outcomes from the workshop demonstrated that, in addition to the levels evident in existing cyber-related exercises within the public and/or private sectors, three cyber exercise levels generally exist:

- national (strategically focused)
- regional (multi-state)
- local (focused on a particular organization)

Whether your audience is public or private will further delineate what types of exercise categories trend. For instance, the military, United States Cyber Command (USCYBERCOM), is known for

two strategic-level cyber exercises (Cyber Guard and Cyber Flag) [DoD 2014, 2016a]. Similarly, the National Guard Bureau (NGB) executes a similar-scale exercise known as Cyber Shield [DoD 2016b]. There are other strategic-level, cyber exercises; however, they are not publicized.

These three government-military, strategic exercises all share a common component: the utilization of a simulated virtual range environment. The Cyber Defense Exercise (CDX) [NSA 2016] is another example involving the same element and often referred to as cyber live-fire exercises (LFX) [Geers 2010] and capture the flag (CTF) [Ghernaouti 2013] competitions. Other government agencies; such as the DHS and Department of Energy (DOE), have their fair share of cyber-related exercises, but unlike those of the military, their cyber-related exercises are often table-top exercises (TTX) [U of W-M 2012] or Functional Exercises (FE – also known as Command Post Exercises) [FEMA 2017b] format driven.

Within a cyber-exercise-level-category, there are different styles of cyber-related exercises. According to SANS [Risto 2015], there are five types:

- tabletop exercises
- online or hosted environments
- simulated and virtual environments
- preproduction testing environments
- penetration tests

When focusing on sector-specific agencies [DHS 2017d], the energy and financial sectors have their own frameworks for executing cyber-related programs. Cyber-related exercises (e.g., Quantum Dawn and Grid Ex) seen within this realm are often national or regionally focused and tailored to a specific sector's needs. Particular to mutual assistance, exercises assist in rehearsing communication flow within command and control structures along with delineating roles and responsibilities. Exercises also serve as a means to experiment, enable innovation and potentially lead to discovery of new possibilities.

2.3.2 Cyber Exercises and Their Role in Cyber Mutual Assistance

The energy sector utilizes the RMAG model to execute command and control of mutual assistance. The RMAG model resembles the Federal Emergency Management Agency (FEMA) Regions Model. There is great interest in exploring cyber mutual assistance concepts through the venue of cyber-related exercises (existing or new). Such exploration is accomplished by identifying the right investment of personnel alongside the development of potential scenario(s). These scenarios would enable the exploration of concepts that potentially lead to solutions impacting the physical and cyberspace domain.

One example of this exploration is in examining "the sharing of skilled and qualified personnel" during a cyber incident. A second example is identifying the equivalent of an Emergency Management Assistance Compact (EMAC) "A-Team." These teams are trained to execute and expedite resource requests and handle the logistics of paperwork and so on. It would be advantageous to have designated personnel for this in cyber mutual assistance. Currently this task is being performed; however, in the aspect of assembling resources for cyber mutual assistance, is there a need to have team(s) of people trained in the process of assembling these resources? This process could include representatives from alternate sources (e.g., the National Guard, DHS, and DoD).

This would enable awareness/visibility of what is happening towards sharing resources and how additional resources can assist or scale up to address a much larger event when additional resources are required.

2.3.3 Recommendations

The CMAW also explored the desire for trying different types of cyber exercises. In all three cyber-exercise categories, scaling becomes an issue with cyber exercises. An organization requires flexibility to identify the types of exercise or wargame needed and the intent and/or goal. The following might be considered: (1) Demonstrate a capability. (2) Identify gaps in order to determine capabilities needed. (3) Exercise command and control decision making. (4) Learn how to prioritize. (5) Develop necessary scenarios to provide participating organizations' awareness, knowledge, and understanding of each other's capabilities. Ultimately, exercises provide a way to enable organizations to be creative and practice collective cybersecurity. Some participant feedback suggested that exercises should be customer/client focused. This could result in improvement of shared best practices.

It's best to periodically test the plan response and processes both theoretically and as a table-top exercise. Cyber exercises should not be limited to a particular category, type, or scope. There is benefit in having variety. However, in matters of scalability, workshop participants noted the need to have more specifically scoped exercises to enable organizations to explore a dilemma, process, or attack scenario in greater detail. This would potentially provide ground truth techniques, tactics, and procedures (e.g., training people on how to respond).

Exercises enable us to explore best practices and how to delineate command and control. One example offered involved the need for more tactical-level or drill-like exercises. One participant shared experiences "examining response to triggers during a Distributed Denial of Service" (DDoS). The benefit of the experience was to develop and capture techniques, tactics, and procedures that "achieve speed, agility and precision." However, there is a challenge in ensuring that there are tools to efficiently capture techniques, tactics, and procedures and update playbooks, standard operating procedures (SOPs), continuity of operations plans, and doctrine. The benefits of conducting cyber-related exercises include "increased awareness of cyber security, improved preparation of staff to handle complex situations confidently, and augment skills of the cyber security team" [Risto 2015].

Over the past decade, cyber-related exercises traditionally began larger in scale. Today, there is an overarching desire to see exercises become more inclusive of cross-sector and public and private participation. The goal is to move smaller and targeted objectives beyond awareness and into testing specific components of interconnected systems. Cyber-related exercises must remain at a relatively small scale to enable flexibility, experimentation, and innovation.

2.4 Rules of Engagement for Operational Technology and Information Technology

During the workshop, the group discussed needed "rules of engagement" around operational technology (OT) and information technology (IT). It is easy to perhaps consider IT and OT as being the same or falling under the same set of management parameters; however they are very different and must be treated and integrated differently from a management perspective [Hayden 2015]. As

mentioned by Hayden, "…IT is key to business of the business—it keeps the information flowing, email running, and databases populated….OT…keeps your power plants running, manages property process lines, and essentially works together to achieve an industrial objective such as manufacturing, transportation of matter, generation of energy, etc." When it comes to management aspects, the IT staff typically work for the chief information officer (CIO). They manage workstations, servers, networking systems, and so forth. The OT staff are typically under the operations, manufacturing, or whatever entity is responsible for the day-to-day operation of the organization. They might be in control of programmable logic controllers (PLC), sensors, valve and motor controllers, relays, and so on. The *NIST Guide to ICS Security* provides a table comparing IT to OT [NIST 2015].

In the past, the OT equipment was not intended to be networked but simply operational; therefore the security aspects necessary for networked equipment were not considered, resulting in inherent vulnerabilities. From a networked perspective, the security aspects did not exist because they were not originally intended to be networked. In terms of patching this equipment to secure a vulnerability, it is typically not as simple as an IT component in that it might have a more significant effect on those who rely on it. Patching an OT system tied to a power substation might cause a power outage for an area versus simply patching some type of IT component where just the network might be down. Obviously, if the power were to go down, then everyone else, including the network that relies on it, would go down as well. Therefore, the logistics involved in patching OT could be much more significant than those involved in patching IT.

According to statistics shared from an interview of industrial control systems vendors, the likeliness of supervisory control and data acquisition (SCADA) systems being patched is low. Approximately 10-20% of companies apply patches to what their SCADA vendors are releasing. This is most likely the result of two factors: (1) There is inherent trust that companies like Siemens are doing everything that needs to be done, but this is short-sighted in failing to appreciate the nuance of company-specific systems. One security firm shared that less than 10% of its customers download the PLC patches. (2) Smaller companies do not have the staff to apply patches. The electricity industry is fraught with old code and technology that is awaiting lifecycle replacement and is basically "unpatchable" until it's upgraded [Higgins 2013].

Security aspects in terms of IT have continued to evolve from the beginning from a networked perspective and, therefore, from a security aspect, IT is a much more mature environment. Therefore, we must have a separate understanding for each when it comes to situational awareness, thresholds, triggers, anomalies, monitoring systems, updates, upgrades, and such. As has evolved in IT, and the ability to establish situational awareness of networked 'IT' systems, we develop secure IT mechanisms for managing and establishing reliable situational awareness from an OT perspective, from manual change analysis to machine learning or artificial intelligence.

From a physical security perspective, operational technology can have a more kinetic or direct effect. As an example, if you modify an OT setting you can cause a generator to spin out of control and cause a fire, cause it to fail, or both. As in the case of Stuxnet, a cyber malware initiated modification of PLC settings modified the spin settings on centrifuges that ultimately resulted in setting back the Iranian nuclear program many years. Similarly, physical security concerns, service provider outages, or other cyber attacks may affect the visibility of network and infrastructure monitoring. One could inject a replay of a normal (or baseline) condition for a power substation

from an IT perspective that is reporting to a higher operations center while physically destroying the substation either via a direct action or via modifying its settings from an OT perspective. Cyber and physical security can be integrated in this regard and therefore the management of both should fall under the same executive. Organizations should also define what traditional operators need to know about cyber security. This includes training, cross-training, "see something say something" type initiatives, and awareness of the difference between operations problems and insider/outsider sabotage type problems, and so forth. It is further necessary to be able to maintain situational awareness of the integrity of the entire system as integrated from an OT perspective into the IT or larger networked system.

This situational awareness includes thresholds and triggers for crosstalk between the IT folks and the OT operators during daily operations, elevated threat, operational anomaly, and resiliency in terms of crisis response, recovery, and prevention mechanisms. This would require an organization to pre-identify the given scope or lanes of IT and OT, and the rules of engagement between the two. Operations monitoring must be fused with IT to maintain that integrity; if they are treated as separate, gaps will occur and may be exploited. When external IT/security help is brought in, then the operations monitoring aspects must be strongly considered regarding how operations are run and integrated into the IT network. Organizations should establish their decision support mechanisms for risk and realized risk. They should also help lead thinking on what should be put in place from a governance perspective for the sake of the industry and the country as a whole.

2.5 What Are the Legal or Regulatory Frameworks to Consider?

Workshop participants were concerned with compliance with all relevant legal and regulatory statutes and frameworks. As is the case with all CIKR protection sectors, multiple levels of legal and regulatory statutes dictate security requirements with varying levels of stringency and compliance mandates. Various federal, state, DoD, and sector-specific regulatory frameworks affect the energy sector, and workshop participants contributed a list of applicable laws, regulations, and standards to which any courses of action prior to and following a cyber event should adhere. The following legal considerations were viewed as being applicable to most parties within the energy sector.

2.5.1 Federal

The Federal Energy Regulatory Commission (FERC) outlines federal rules that regulate the interstate transmission of electricity, natural gas, and oil, and provide the overarching regulatory guidelines that govern the energy sector. Beyond FERC regulation, there is some applicability of the Stafford Act as it pertains to Environmental Protection Act (EPA) waivers during declared major disasters and emergency assistance [FEMA 2017a]. This may dictate response actions should a cyber attack have significant environmental impact and lose some environmental protection regulations when certain disaster conditions are met. With regards to energy corporation size and control, federal antitrust and Federal Trade Commission (FTC) regulations aim to maintain sector competition and protect American consumers. With regards to cybersecurity, the DHS critical infrastructure sectors are often pointed to the National Institute of Standards and Technology's (NIST) guidelines, standards, and frameworks in order to provide a federal standard for asset security across sectors.

2.5.2 Department of Defense

Of interest to participants in light of the workshop's cyber mutual assistance focus were the conditions to be met and expectations that would arise should the energy sector suffer such dramatic degradation that the DoD is tasked to aid in response in accordance with Joint Publication 3-28 (JP 3-28) Defense Support to Civil Authorities. According to JP 3-28 and DoD Directive 3025.18 (DODD 3025.18), if certain conditions are met under which a civil authority requests immediate response, the DoD (with approval through the Chain of Command) may be used to provide immediate support until such time as sufficient federal, state, local or other agency resources are available to adequately respond. With regards to a cyber event widely affecting the energy sector that may degrade basic utilities to the state of an emergency, it is possible that DoD Cyber Mission Teams (CMT) may be used to assist. However, the clearance for such support is held at the Secretary of Defense or Presidential level, so other response agencies may be more likely to assist, such as those from the DHS or a state's National Guard force.

2.5.3 State

Much of the applicability of state legal and regulatory statutes involves the use of the National Guard under Title 32 authorities as an option for Defense Support to Civil Authorities under State officials' authority. With the development of National Guard Cyber Protection Teams (CPTs), we may see more Title 32 cyber support; however, DODD 3025.18 still governs their use and limits the conditions and duration of their use the same as federally controlled forces. While much of the transmission of energy commodities may be across state boundaries, there are cases where state level antitrust acts may apply to energy sector corporations.

2.5.4 Energy Sector Specific

Specific to the energy sector are applicable North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards that cover different domains of asset, information, system, physical, and personnel security as well as incident reporting and response plans. Workshop attendees also mentioned the usefulness of the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), which was authored by the DOE with the purpose of addressing the unique cybersecurity characteristics of the electricity subsector. The ES-C2M2 model can be used by energy sector entities to self-evaluate, measure, and improve their own cybersecurity programs. It is targeted to organizations of all sizes, and nests nicely as a tool for implementation of the standards outlined in the NIST Cybersecurity Framework (CSF).

2.6 General Cyber and Physical Security

In general, the workshop highlighted the various best practices and principles that can help to mitigate risks within the energy sector. While the SANS Institute's Critical Security Controls were mentioned as a worthwhile resource, general guidelines that govern an organization's processes and procedures for cybersecurity incident response and customer data privacy were also deemed important for effective preparation for an incident. Furthermore, processes for employee security clearance, non-disclosure guidelines, employee safety, and applicable safety regulations regarding physical protection systems were also highlighted as areas that required attention as risk control measures.

Beyond the aforementioned legal and regulatory frameworks, other frameworks, programs, and legal statutes were less well-known, or seen as requiring further investigation as to how they would affect the energy sector as it pertained to cyber mutual assistance and incident response. For example, the U.S. Nuclear Regulatory Commission (NRC) has its own cybersecurity requirements that pertain specifically to nuclear power plants, as well as its own regulations listed in U.S. NCR Regulatory Guide 5.71. Other NRC documents, such as its 2014-2018 NCR Strategic Plan, highlight cybersecurity as a major factor in ensuring the safety of nuclear power production. Other programs exist that ensure electricity distribution can be rapidly restored, such as the Spare Transformer Equipment Program (STEP) and SpareConnect program outlined by the Edison Electric Institute. These programs encourage service providers to acquire and maintain spare components critical to energy distribution and streamline the ability to share those components in the event of an emergency. Having these parts on hand can greatly reduce the time in which services can be restored after an incident. STEP and SpareConnect are more physical bench stock forms of mutual assistance.

Breach and compromise notification requirements, especially to federal regulators, were mentioned by participants as an area where further study of existing statutes was required before building mutual assistance courses of action. Other frameworks were discussed as they pertain to cyber and physical risk assessments, applying to organizations beyond just the energy sector, such as the Federal Financial Institutions Exam Council (FFIEC) Cybersecurity assessment and NIST Cybersecurity Framework, both of which can help to assess the current maturity of a cybersecurity program. The ES-C2M2 was again mentioned as an energy sector focused framework for assessing cybersecurity posture within the sector. Workshop participants also discussed the North American Reliability Corporation's (NERC) Protecting Critical Infrastructure Information (PCII) [DHS 2017f]. Program as a good source document for explaining details of energy sector information. Finally, the Cybersecurity Information Sharing Act, passed in December 2015, arose as a topic that required further study as to how cybersecurity information sharing would increase in the future between organizations, CIKR sectors, and between the DHS and industry.

2.7 What Skillsets Are Required (IT/OT)?

One of the most involved discussions during the workshop focused on *Asset/Talent Management/Workforce Development* perspective. Detailed discussion took place regarding the current skillset gap that must be addressed for a cyber mutual assistance agreement (CMAA) to be successful.

The DHS National Initiative for Cybersecurity Education (NICE) developed the Cybersecurity Workforce Framework (currently in version 2.0) under the Department of Homeland Security (DHS) National Initiative for Cybersecurity Education (NICE). The Cybersecurity Workforce Framework (2.0) [DHS 2017e] defines seven categories shown in the slide. These map to 31 specialty areas (each with typical job titles, tasks, and KSAs). The Cybersecurity Workforce Framework defines seven categories of work. These are listed below:

- analyze
- investigate
- operate and maintain
- protect and defend

- securely provision
- oversight and development

These seven categories map to 31 specialty areas, each with typical job titles, tasks, and knowledge, skills, and abilities (KSAs). We grouped the CMAW participant responses under these categories in response to this question: What skillsets are required in a CMAA? Our intent was to determine which skillsets mapped directly to the workforce framework and which represent skillsets unique to cyber work in the power sector.

The workshop participants provided a total of 65 skillsets, which were pared down to 52 after elimination of duplicates. Of these, a majority (30) of the responses fit well within the Cyber Workforce Framework. Since this framework already describes these skills in detail, we performed no further analysis of them and simply list them under the appropriate categories, providing the corresponding data element code and label (denoted as numbers in "[ ]"). It is noteworthy that the protect and defend category contains almost half of the responses in this section.

2.7.1 Analyze

- cyber threat analysis [14 – Threat Analysis]

2.7.2 Investigate

- digital forensics training (chain of custody, evidence retrieval) [21 – Digital Forensics]
- image capture [21 – Digital Forensics]
- industrial control system specific forensics [21 – Digital Forensics]
- reverse engineers [22 – Investigation]
- malware analysts [22 – Investigation]
- collect and operate
- threat actor hunting [32 – Cyber Operations]
- sensor management [31 – Collection Operations]

2.7.3 Operate and Maintain

- database expert [42 – Data Administration]
- knowledge management [43 – Knowledge Management]
- telecommunications network engineer [44 – Network Services]
  - CISCO
  - telephony
  - fiber optics
- system integration [46 – System Security Analysis]

2.7.4 Protect and Defend

- event logging analysis [51 – Network Defense Analysis]
- protocol analysis [51 – Network Defense Analysis]
- data log analysis [51 – Network Defense Analysis]

- net flow analysis [51 – Network Defense Analysis]
- system analysis [51 – Network Defense Analysis]
- operating system hardening [52 – Infrastructure Support]
- incident response [53 – Incident Response]
- emergency response [53 – Incident Response]
- business continuity [53 – Incident Response]
- intrusion analysis [53 – Incident Response]
- cyber risk analysis [54 – Vulnerability Assessment and Management]
- ethical hacking [54 – Vulnerability Assessment and Management]
- red teaming [54 – Vulnerability Assessment and Management]

2.7.5 Securely Provision

- compliance [61 – Compliance]
- development operations [63 – Systems Development]

2.7.6 Oversight and Development

- legal [73 – Legal Advice and Advocacy]
- backup [74 – Security Program Management]
- Information Systems Security Plan (ISSP) [74 – Security Program Management]

The participants also identified 10 operational technology (OT) skillsets that do not fit within the Cyber Workforce Framework. These would require additional analysis in order to determine the capabilities required to perform the work in the context of a CMAA. It is telling that, while some responses dealt with traditional OT, others (e.g., transmission network analysis) included skills in managing the effects of OT on physical systems. The responses are listed below without further discussion.

- OT and programmable logic controller (PLC) configuration engineers
- SCADA system operations
- industrial control system (ICS) and National Incident Management System (NIMS) understanding
- Distributed Network Protocol (DNP)
- Global Information Assurance Certification (GIAC) Global Industrial Cyber Security Professional (GICSP)
- transmission network analysis
- protective systems engineers
- reliability coordination on restoration
- Department of Energy Secure Power Systems Professional (SPSP)
- station operators

Finally, and perhaps most tellingly, the workshop participants provided 12 other skills that would be needed in a CMAA, but do not fall within traditional IT or OT skillsets. Some of these responses might be indicative of systemic or procedural shortcomings, rather than anticipated personnel shortages in times of cyber attacks on power systems.

- Leadership integrated capabilities: This pertains to the ability to lead integrated teams during response operations. It should not come as a surprise that seasoned leaders with response experience would be in high demand during a cyber event of consequence.
- Command and control: Related to the leadership point above, this skill is more focused on the process of coordinating and synchronizing the response activities, rather than providing leadership.
- Soft skills to bridge engagement between IT/OT: Technical staff in these two specialty areas have different perspectives that can become points of friction during a response operation. Having additional personnel skilled at bridging these communities could help remove obstacles and restore services more quickly.
- Facilities safety: We presume that with additional personnel in multiple facilities trying to quickly restore services, normal safety measures may be insufficient.
- Vendor management: Personnel with these skills would be those who are adept at rapid contracting and acquisition actions, as well as those who can quickly evaluate proposed vendor solutions.
- Crisis communications and public relations: The communications team is often overlooked during the initial response, which can lead to bad press and loss of trust for the organization in the critical first hours.
- Scribing abilities that involve multiple inputs and track timelines: Those who have experienced cyber events of significance would likely vouch for the requirement to have a skilled and detail-oriented scribe documenting all actions taken by the responders.
- Analytical skills: This skill was not further explained by the participant, but is worth listing distinctly from the other, more specific, analytical skills mentioned above.
- Baselining skills: This is another vaguely stated skill, but it would be reasonable to assume that it would not be as useful during the response as it would be prior to the incident.
- Addressing spares requirements: Presumably, this entry refers to the management of spare parts. Like the lineman [BLS 2017] entry before it, this may not be well suited for a cyber response.
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) [NERC 2016]

While the skillsets identified by the participants across all categories of work are insightful, some are not actionable without further analysis. The OT skills identified could be further refined by developing use cases or scenarios in which one might better glean the manner in which these skills might be employed. The final category of miscellaneous skills is perhaps most useful for identifying internal gaps that must be addressed before the crisis, rather than as gaps to be filled by a partner organization during execution of a CMAA.

2.8 What Is Your Understanding of Cyber Mission Forces (CMF) and How Can They Help?

Another area of discussion involved the participants' current understanding of the Cyber Mission Force (CMF). Overall feedback from the audience demonstrated a desire to learn more about the CMF mission its capabilities. Does the CMF possess capacity to directly assist with a private or public sector incident response situation? To help answer such questions and to gain context regarding where the CMF might be effectively employed, it is best to refer to the April 2015 Department of Defense Cyber Strategy. Within this document, the DoD specifies three primary cyber missions. The first cyber mission is to defend DoD networks, systems, and information. The second, most applicable mission to this workshop is to defend the U.S. homeland and U.S. national interests against cyber attacks of significant consequence. As it encapsulates more than the DoD, this is the broadest mission. The third cyber mission is to provide cyber support to military operational and contingency plans. Within the Cyber Mission Force construct there are varying types of teams with different roles and capabilities. There are national teams, whose purpose is to focus on national-level assets and or incidents. There are service-specific teams that focus on service-specific (Army, Navy, Air Force, and Marine) assets and or incidents. Lastly, there are combatant command teams whose purpose is to directly support a geographic combatant commander. At each level, be it national, service, or combatant command, there are generally three types of teams: offensive, defensive, and finally, supportive in nature.

The defensive arm of the Cyber Mission Force is made up of Cyber Protection Teams (CPTs) that are charged with the responsibility of defending priority DoD networks and systems against priority threats. Unique to Cyber Protection Teams at the national level is an intent to directly align teams with CIKR sectors. Cyber Protection Teams possess a wide range of skills, which include, but are not limited to, the following: the surveying of cyber key terrain, incident response, adversary hunting, vulnerability assessment, and penetration testing. Given the current state of the CMF, there is interest in increasing and growing cyber capacity, which would facilitate support across all CIKR sectors. In order for this growth initiative to be successful, the CMF should engage, when appropriate, with the public and private sector to prioritize and to identify training gaps and areas of specialization that are most required.

Can the Cyber Mission Force directly assist in response to a cyber attack against a CIKR sector? U.S. Cyber Command has authority and responsibility over the Cyber Mission Force and can approve where a team may be deployed or how it is utilized. Until legal and policy frameworks are clearly in place, private and public CIKR sector companies should continue to work with the DHS and Federal Bureau of Investigations (FBI) for requested cyber assistance. As part of a whole of government approach, it stands to reason that U.S. Cyber Command works closely with the DHS, the FBI, U.S. CERT and other key governmental agencies in order to synchronize threat intelligence and defensive cyber operations. It is important to reiterate that the DoD has a scoped and specific role when it involves cyber attacks against the nation and CIKR. In the future, as allowed by policy, a desired end state is to have a responsive framework for both CMF and CKIR sectors to collaborate and to learn from each other. Once this framework is in place, it will pave the way to address the workshop's additional questions and concerns about trust, confidence, threat intelligence sharing, data sharing, and data retention with the DoD. How knowledgeable are CMF teams with regard to power and electric IT and OT? As a starting point, the barrier to trust and confidence can be overcome through continual dialogue, collaboration, and exercise. Cyber exercises

such as Cyber Guard and Cyber Shield are great opportunities for CMF teams to demonstrate capability and to train with its potential partners from industry. Just as the CIKR sectors must prioritize their network assets and systems that require protection, the same must be done with the CMF in how it approaches its relationship building and partnering.

Recommended Way Forward: Both the CMF and CIKR sectors have much to learn about each other in the cyber space domain. In order to maximize responsiveness and to effectively mitigate a serious cyber attack against the nation and any of its CIKR sectors, the establishment of key relationships must be a priority. First and foremost, there should be increased opportunities for collaboration under a clear framework that is grounded in approved policy. After this milestone is achieved, codification of detailed agreements can begin, which would allow and define direct engagements that could occur. This could potentially include cross training, sharing of technology, and tactics, techniques, and procedures. The Army Cyber Institute is a resource that should be leveraged to help engage and to prioritize partnerships and relationship building in this domain.

2.9 Pre-Incident Preparation

In a previous research question involving desired skillsets, the participants identified the "what" that is needed to assist the cyber mutual assurance effort. In the pre-incident preparation discussion, the participants discussed the "how" and examined common topics across the power sector that are important to each stakeholder. It is relevant and worthy to mention the NIST Framework for Improving Critical Infrastructure Cybersecurity [NIST 2014]. Within this document, NIST describes a core framework that gives general guidance on how to achieve cybersecurity outcomes with respect to incident response and preparation. The core functions of the Cyber Security Framework are to Identify, Protect, Detect, Respond, and Recover. These core functions, when combined with the NIST Incident Response Methodology steps—Preparation; Detection and Analysis; Containment, Eradication, and Recovery; and, lastly, Post Incident Activity—provide great context for establishing common standards, procedures, and terminology across both industry and the DoD. Preparation is further defined as both the establishment of incident response capability, but also measures needed to prevent incidents by ensuring that systems, networks, applications, are sufficiently secure.

The top categories brought up for discussion under incident response preparation with participants were the following: recovery and resiliency, asset management and prioritization, establishment of SOPs, common and cross training opportunities, and lastly the need for a cyber mutual assistance playbook.

Recovery and resiliency with respect to the power and energy sector are arguably the most important goals of cyber incident response and preparation. The positive side to recovery and resiliency is that there are similarities and procedures already in place in some regions for dealing with natural disasters. The notion of having backups (gold disks) and failover redundancy is common, although still very critical to restoring services and bringing systems back online quickly. A common technique used in this sector is to ensure that spare/clean hardware is readily available to swap out if primary hardware is compromised or damaged. Having a prepositioned stock of equipment with a transportation plan supports this technique as well. The fact that some equipment is very old and or considered legacy should also be factored into resiliency. What systems have or do not have a manual failover implementation? Another key point for recovery is understanding the connectedness of critical equipment and their dependencies. Resiliency planning

must be built into all systems, processes, facilities, and within people as well. With cyber mutual assistance, the ability to rely on and to reach out to partners for expertise, spare equipment, and or services greatly increases capacity for both recovery and resiliency.

Asset management is a concept applicable to everyone as it applies to incident response preparation. Having accurate documentation and access to a current status of assets is critical for both situational awareness and for conducting daily operations. Artifact examples include network diagrams, infrastructure plans, configuration details, software and system baselines, patch management systems, and vendor information. Furthermore, it is the prioritization of these assets that should be done in order to develop cost-effective risk management and mitigation techniques. The most important and critical systems should have the most defense and or security measures in place, such as sensors, logging, and auditing. Additionally, prioritization should be applied to the process and the order in which systems and services are restored. Unique to the power and energy sector is the recommended separation of IT and OT during conducting of asset management prioritization. Shared understanding of this separation will help streamline responses during an incident response event, while also clearly delineating impact caused by an incident. There is also merit to the separation of duties for personnel with IT and OT roles because having single of points of failure is not a best practice.

The establishment of a cyber incident response SOP or action plan is critical to incident response preparation. Having established pre-planned and pre-approved actions within an SOP can greatly improve mitigation and response time when dealing with an incident. It is important to have an established communication plan that utilizes both in and out of band channels. This serves as a means for ensuring redundancy but also for maintaining security should a primary band be compromised or down. Incident responders need to know whom to contact and how, both internally and externally. Creating pre-templated contact cards and telephone trees with call criteria can ensure effective command and control. Another key consideration for planning is how to communicate with a large customer base in the event of an incident.

With incident preparation, it is worthwhile to identify common training required for incident responders. An important discussion around this topic involves quantity versus quality, and specialization versus flexibility. In a perfect scenario, an organization might have a deep bench of quality personnel when it comes to a specialized skillset. A general assumption is that it will be harder to find and to train specialized personnel, and this is where more attention should be placed with respect to training. Having more flexibility or more generalists on your team is not necessarily negative, but overall composition should be carefully considered. Having a common training pipeline for incident responders ensures sustainability, repeatability, and compatibility. Training in turn should be prioritized to help focus on vulnerable areas. As partnerships are developed between companies, cross training is an opportunity to increase understanding of each other’s capabilities and to create trust and confidence. Companies need to rigorously exercise their incident response SOPs and action plans. Additionally, where possible, companies should look for opportunities to train with local responders, law enforcement, and state emergency centers. A final recommendation for mutual assistance and preparation is to form a pool of expertise that may support a region or group of power companies. The intent would be to rapidly deploy people from this pool to quickly surge on an incident.

During this discussion, many participants recommended that a cyber mutual assistance playbook be created. This playbook would serve to complement the national framework and not replace an incident response SOP or action plan, but rather give further details and guidance on how to execute mutual assistance. Within this playbook some potential chapters might include the following:

- legal and nondisclosure agreements
- human resource considerations
- specifications on what a mutual aid team might look like
- a standard brief for external support members to quickly understand the environment
- a support plan and package for a mutual aid team
- key resources for collaboration and information sharing(e.g., Electric ISAC membership and portal)

2.10 What Are the Critical Assets?

One of the most important steps in building a resilient system is the identification of critical assets. The group participated in an initial brainstorm of critical assets. Any system, process, people, equipment, data, and so forth, that are required to keep the lights on is considered a critical asset. It becomes extremely important to know your environment.

This starts with understanding your equipment. What are the most critical pieces of equipment in your organization, such that if you do not have them for a length of time you cannot complete the mission? As part of this understanding you need to keep abreast of, or have a process in place on, their supply chain management from cradle to grave. This includes who manufactured the equipment (when and where) with what components (when and where)—all the way to if it fails—then what is the process, cost, and time for replacing it. This information is sensitive, and if adversaries gain this information then they've completed the first step in being able to conduct nefarious activities on your organization. Along the way you will have to keep this equipment updated, patched, and maintained. Obviously this situational awareness is not the responsibility of a single person, which would be intractable. However, as stated, it is very important to have a process in place for all of your equipment, but starting with the most important from a mission accomplishment and resiliency aspect. Complicating factors include a piece of equipment that might be considered so critical that you do not want to take it offline to patch or integrate into an exercise scenario. It is extremely important for the organization to consider this possibility and how it would deal with this aspect as part of its risk assessment.

Having the right personnel and the talent management of personnel for the organization to manage or conduct the systems, process, equipment, and data is imperative. This includes the right IT folks for those applicable IT positions from networking to network management and analysis to OT with ICS/SCADA and other necessary and applicable expertise. Most important is having the expertise to be able to develop and integrate processes across the organization such that the gaps of where one skill ends and another begins are covered. Talent management is often overlooked when it comes to the lifecycle of an employee from pre-hiring to termination. It should be strongly considered when it comes to hiring, termination, retaining, training, and leading.

An organization's processes and tools are critical assets for synchronizing the leadership with the personnel and equipment as well as with outside agencies, vendors, and government. These include the techniques, tactics, and procedures that are in place for individuals to do their jobs, but, more importantly, are the processes in place that keep the separate areas synchronized and the cover down on gaps between them. The intent is to achieve defense in depth; consider what your critical assets are able to do that is not limited to redundant communications, logging, back-ups, network monitoring and related processes, forensics, lifecycle and patching updates, STEM systems, capturing systems, contractual and legal paperwork for external mutual assistance, (Cyber) Security Centers, payroll system processes, incident response, and resiliency plans.

One of the most important steps in building a resilient system is the identification of critical assets. The group participated in an initial brainstorm pertaining to critical assets.

2.11 Sources of Threat Information

Threat modeling is a vital component of risk assessment processes and business continuity planning and is important to prioritizing resources and control measures for an organization's security management architecture. It is a process that enables the prioritization of countermeasures, which is particularly important in a resource-constrained environment. In order for security personnel to perform effective threat modeling, however, the organization must have access to high-quality threat feeds that are relevant to the company's environment, to inform the decision making process. During the workshop, participants discussed a variety of sources from which this vital information is drawn.

As discussed by the contributors, the primary source of threat intelligence for any given network comes from within the company's or agency's internal network. These functions are usually performed by security administrators and IT staff during the performance of their daily duties. One of the primary functions of these personnel is to establish accountability among users by auditing their activities and limiting their behavior. During this process, valuable information is collected about the network that helps administrators understand threats against their networks. This information is collected through network logs (system, application, and firewalls), sensors, investigations, forensics, and lessons learned. Security personnel can also receive valuable threat information by monitoring chat rooms, conducting research on the dark web, or following cybersecurity-related news. Workshop members identified other threat intelligence collection sources during the workshop, which are discussed in greater detail below, categorized by source.

2.12 Public Sector Threat Intelligence

The DHS is the designated cybersecurity coordinator for the U.S. public and private sector and is a valuable source of threat intelligence for both groups. Therefore, subordinate DHS groups like the United States Computer Emergency Readiness Team (US-CERT) aggregates and disseminates routine threat information to all members of the 16 designated Critical Infrastructure (CI) sectors, using standards such as the Structured Threat Information eXpression (STIX™), the Trusted Automated eXchange of Indicator Information (TAXII™), and the Cyber Observable eXpression (CybOX™) to standardize and exchange threat information throughout the industry [DHS 2016c]. As directed by E.O. 13549, the DHS Private Sector Clearance Program and Cyber Information Security Act (2015) seek to remove barriers that prohibit the sharing of this valuable information to designated partners.

Industrial Control Systems (ICS)-CERT, also internal to the DHS, monitors threats and vulnerabilities specifically related to ICS systems that are often used to regulate large-scale power grids, water processing facilities, and a variety of other critical infrastructures. The DHS has a variety of other offices that provide valuable information to the private and public agencies that it supports, but US-CERT is the primary organization through which agencies can interface with the whole of DHS cyber threat intelligence efforts.

Additionally, sector specific regulators, such as the FERC, collect actionable intelligence on a routine basis, which they use to adjust regulation requirements for the energy sector. Through audits and inspections, this information is passed on to community members.

Other public agencies and resources mentioned as sources of threat intelligence include the following:

- local law enforcement (e.g., NYPD Cyber Intelligence and Cyber Crimes)
- State Federal Management Threat and Heard Identification Risk Assessment (THRIA)
- Federal Emergency Management Agency (FEMA) and other natural disaster agencies
- The FBI Cyber Division
- Department of Treasury
- Department of Energy
- The intelligence community (limited access)

2.13 Industry Forums and Groups

The private sector interfaces with the government agencies, usually US-CERT, through privately formed entities known as Information Sharing and Analysis Cells (ISACs). Each of the designated CI sectors has some form of an ISAC that serves as the mechanism through which information is collected and shared throughout a particular sector, both internally and with the public sector.

Two ISACs were of particular focus for this working group: (1) the Electricity-ISAC (E-ISAC) and (2) the FS-ISAC. According to its website, the E-ISAC collaborates with the Department of Energy and the Electricity Subsector Coordinating Council to serve as the primary security communications channel for the electricity subsector. The Financial Services-ISAC (FS-ISAC) provides a similarly critical role for the financial services sector.

Public-private sector partnership are not limited to interactions through the ISACs. InfraGard, for instance, is a public-private sector partnership between the FBI, corporations, and a variety of other public agencies. InfraGard is designed to help participants share intelligence to prevent hostile acts against their infrastructure [InfraGard 2016].

2.14 Cybersecurity Vendors

The final category of intelligence providers includes private vendors that deliver security as a service or product. During the workshop, members discussed two primary sources of security services through which security professionals can derive intelligence for their networks: System Information and Event Management (SIEM) products and threat intelligence products.

Security analytics and SIEM products usually include a variety of hardware and software applications within the organization's network that continuously monitor and analyze network and system activity to provide situational awareness for security professionals and network administrators. SIEM products such as Splunk provide administrators with a real-time picture of what is occurring on their networks.

Given the evolutionary nature of the threat, however, security professionals can no longer merely be concerned with the activities internal to their networks; they must also be externally focused. Threat intelligence enables organizations to have insight into threat activity that has not yet touched their networks and to anticipate the threat's behavior. Thus it allows them to become more proactive and less reactive.

The threat intelligence market is poised to grow 14.3% between 2015 and 2020. The members discussed some of the market's biggest players:

- ThreatConnect
- FireEye/ iSight
- Palo Alto Networks
- Crowdstrike
- Looking Glass Cyber Solutions
- SecureWorks
- AlienVault

For a fee, these firms offer real-time threat information in structured data formats and often place SIEM or Intrusion Prevention Systems (IPS)/Intrusion Detection Systems (IDS) on their clients' networks to supplement their intelligence services. Other vendor solutions include "freemium" services that are made available to the public at no cost. IBM's X-Force capability, for instance, provides similar features to the platforms above, as does ThreatCrowd. Like the paid services above, many of these platforms aggregate crowd-source threat intelligence and SIEM data to inform its users about current threat trends.

There is a large variety of sources from which organizations can draw threat intelligence. In order to be most effective, cybersecurity experts must effectively analyze each feed and discern which provide intelligence that is most relevant to their organization.

3 Conclusions and Recommendations

The CMAW was extremely valuable in defining the multiple perspectives that are part of developing a successful long-term private-public partnership program. The discussions surrounding each of the various research questions provided insight into the challenges the ACI faces around developing and implementing the processes and procedures necessary to advance partnerships, establish governance and oversight, and prepare for a rapid response in the event of a cyber attack.

The following set of recommendations warrant consideration:

1. Examine additional study and testing of hypotheses identified in this workshop through exercises with industry partners and stakeholders.
2. Develop a detailed workforce development plan based on the skills defined above to ensure proper resourcing.
3. Define and understand existing applicable policy and strategy (including legal and funding implications) for standing up cyber RMAGS.
4. Identify areas of opportunity for joint cyber missions and capabilities with the Army Cyber Institute and infrastructure industry companies.
5. Conduct an experiment such as a cyber exercise. The exercise will provide a use case to enable further research of cyber mutual aid and potentially help to evolve cyber multi-sector regional exercises.

One of the CMAW overall objectives was to discuss multi-sector exercise development. As a result the ACI will conduct a follow-on experiment as phase two of overall research to examine interdependencies among sectors [DHS 2017c].[3] Over the next month, the ACI will begin developing a small cyber multi-sector exercise. The exercise will be designed to encourage (if not require) inter-sector coordination in order to mitigate the effects of a phased cyber attack. Objectives are below:

- Encourage business unit leaders and technical responders to work collaboratively.
- Focus on information sharing and response coordination. Developed scenarios will stress inter-sector information sharing and the NYC Emergency Management prioritization and coordination of recovery effort.
- Examine interdependencies, identify the potential gaps between sectors and challenges to cyber security. Identify strengths and weaknesses and potentially draw out best practices for improving system security and incident response.
- Provide awareness and insight to challenges facing sectors as it pertains to responding to a cyber attack.

[3] Department of Homeland Security (DHS) definition of 16 critical infrastructure sectors: Emergency Services, Financial, Energy, Healthcare/Public Health, Communications, Dams, Transportation Systems, Water/Wastewater Systems, Information Technology, Nuclear Reactors, Materials/Waste, Defense Industrial Base, Critical Manufacturing, Food/Agriculture Government Facilities and Chemical, Commercial Facilities. See https://www.dhs.gov/critical-infrastructure-sectors

Appendix A List of Abbreviations, Acronyms, and Definitions

Anti-Trust Acts Sherman Act outlaws "every contract, combination, or conspiracy in restraint of trade," and any "monopolization, attempted monopolization, or conspiracy or combination to monopolize." Federal Trade Commission Act, bans "unfair methods of competition" and "unfair or deceptive acts of practices." Clayton Act addresses specific practices that the Sherman Act does not clearly prohibit, such as mergers and interlocking directorates [FTC 2017].

Capture the Flag (CTF) is a concept used to train or as a competition. Demonstrating real-life exploits in the field of breaking security protection and knowledge exchange of information technologies and techniques, DEF CON is one of the oldest, largest and most popular hacker conventions that offer cyber CTF competitions. The term *Capture the Flag* refers to American games, multimedia or non-multimedia, where the objective is to capture and to plant a flag, symbolically, in the same way as the first man on the moon did on July 20, 1969 [Ghernaouti 2013].

Carnegie Mellon University|Software Engineering Institute|Cyber Emergency Response Team (CMU-SEI-CERT) is a is a division within Carnegie Mellon University and the Software Engineering Institute (SEI) that studies and solves problems with widespread cybersecurity implications, researches security vulnerabilities in software products, contributes to long-term changes in networked systems, and develops cutting-edge information and training to help improve cybersecurity. The CERT Division works with the DHS on goals in data collection and mining, statistics and trend analysis, computer and network security, incident management, insider threat software assurance, and more [SEI 2017b].

CERT Resilience Management Model (RMM) has two primary objectives: (1) establish the convergence of operational risk and resilience management activities such as security, business continuity, and aspects of IT operations management into a single model, and (2) apply a process improvement approach to operational resilience management through the definition and application of a capability-level scale that expresses increasing levels of practice maturity [SEI 2017a].

Certified Ethical Hacker (CEH) is a skilled professional who understand and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s) [EC-Council 2017].

Certified Information System Auditor (CISA) is a globally recognized certification for IS audit control, assurance, and security professionals. Being CISA certified showcases audit experience, skills and knowledge, and demonstrates capability to assess vulnerabilities, report on compliance, and institute controls within the enterprise [ISACA 2017].

Cooperative Research and Development Agreement (CRADA) is a legal agreement between a federal laboratory and one or more nonfederal parties such as private industry and academia. These agreements offer both parties the opportunity to leverage each other's resources when conducting research and development that is mutually beneficial [ARL 2017].

Critical Infrastructure Cyber Community (C3) Voluntary Program. The U.S. depends on critical infrastructure every day to provide energy, water, transportation, financial services, and other

capabilities that support the country's needs and way of life. This program supports owners and operators of critical infrastructure, academia, federal government, state, local, tribal, and territorial (SLTT) governments and business in their use of the NIST Cybersecurity Framework [DHS 2017b].

Cyber Defense Exercise (CDX) is an annual competition, mounted by NSA information assurance experts, that tests skills in building, securing, and defending networks from hostile attacks. The Information Assurance Directorate (IAD) sponsors and collaborates with organizations across NSA to conduct the competition, held annually since 2001 [NSA 2016].

Cyber Guard is a U.S. Cyber Command exercise, evolving and continually expanding to meet the demands of the Department of Defense and the nation. Cyber Guard 12 was developed to foster coordinated cyberspace incident responses between the federal and state governments, exploring the National Guard's potential as an enabler and "force multiplier" in the cyberspace domain [DoD 2016a].

Cyber Flag is a U.S. Cyber Command, Joint and coalition cyberspace force-on-force training exercise, fusing attack and defense across the full spectrum of military operations in a closed network environment [DoD 2014].

Cyber National Mission Force (CNMF) is designed to defend DoD information networks, support combatant commander missions and defend the nation's critical infrastructure. The force will eventually be made up of 133 teams, which will give the department a means to apply military capability at scale in cyberspace [DoD 2016b].

Cyber Shield is a defensively focused cyber exercise that is designed to develop, train, and exercise National Guard cyber-capable forces, Cyber Network Defense Teams (CND-T), threat analysis teams, reporting mechanisms, and leaders. The purpose of the exercise is to provide a collective training event for the evaluation of CND-Ts and to set the conditions for team validation [DoD 2016c].

Cybersecurity Capability Maturity Model (C2M2) was derived from the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) Version 1.1 by removing sector-specific references and terminology. The ES-C2M2 was developed in support of a White House initiative led by the Department of Energy (DOE), in partnership with the Department of Homeland Security (DHS), and in collaboration with private- and public-sector experts [DOE 2017].

Cybersecurity Risk Information Sharing Program (CRISP) is a public-private partnership, co-funded by the U.S. Department of Energy's Office of Electricity Delivered and Energy Reliability (DOE/OE) and industry. CRISP establishes a partnership between DOE/OE, the North American Electric Reliability Corporation's (NERC) Electricity Sector Information Sharing and Analysis Center (ES-ISAC), Pacific Northwest National Laboratory (PNNL), Argonne National Laboratory (ANL), and participating companies. The purpose is to collaborate with energy sector partners to facilitate the timely bi-directional sharing of unclassified and classified threat information and develop situational awareness tools to enhance the sector's ability to identify, prioritize, and coordinate the protection of their critical infrastructure and key resources [ISACA 2017].

Defense Support to Civil Authority (DSCA), in accordance with the Department of Defense Directive 3025.18, authorizes immediate response authority for the use of military force (applies to

the Army National Guard and Air National Guard), under situations. Federal military commanders are provided EMERGENCY AUTHORITY under this Directive. Federal military forces shall not be used to quell civil disturbances unless specifically authorized by the President in accordance with applicable law ...or permitted under emergency authority [DoD 2013].

Defense Production Act (DPA) states that the security of the U.S. is dependent on the ability of the domestic industrial base to supply materials and services for the national defense and to prepare for and respond to military conflicts, natural or man-caused disasters, or acts of terrorism within the U.S. The Defense Production Act of 1950, as amended [50 U.S.C. App 2061 et seq.]

U.S. Department of Homeland Security (DHS) Definition of 16 critical infrastructure sectors: Emergency Services, Financial, Energy, Healthcare/Public Health, Communications, Dams, Transportation Systems, Water/Wastewater Systems, Information Technology, Nuclear Reactors, Materials/Waste, Defense Industrial Base, Critical Manufacturing, Food/Agriculture Government Facilities and Chemical, Commercial Facilities [DHS 2017c].

Distributed Energy Resources (DER) are smaller power sources that can be aggregated to provide power necessary to meet regular demand. As the electricity grid continues to modernize, DER such as storage and advanced renewable technologies can help facilitate the transition to a smarter grid [EPRI 2017, FEMA 2017c].

Distributed Environment for Decision-Making Exercises – Financial Sector (DECIDE-FS) is a Norwich University tool that was developed under a $9.9 million contract awarded in 2013 by the Cyber Security Division of the DHS Security Science and Technology Directorate. The only tool of its kind, DECIDE-FS was initially designed to test U.S. financial sector cybersecurity and can be adapted for use in other critical infrastructure arenas, such as utilities and communications. The platform replaces simple tabletop exercises with a business simulation customized to individual business models, information technology topology, and organizational dependencies. In the exercises, built over a financial markets simulation, business leaders are stressed with cyber threats that affect the markets—price, volume, latency, and utilities, as well as how each organization is structured in terms of business model, value chains, and dependencies [Norwich University 2015].

Distributed Network Protocol (DNP3) is a set of communications (layer 2) protocols used between components in process automation systems. Its main use is by utility providers, such as electric and water companies. Use in other industries is not common. It was developed for communications between various types of data acquisition and control equipment. DNP3 plays a crucial role in SCADA systems, where it is used by SCADA Master Stations (also known as Control Centers), Remote Terminal Units (RTUs), and Intelligent Electronic Devices (IEDs). It is primarily used for communications between a master station and RTUs or IEDs. ICCP, the Inter-Control Center Communications Protocol (a part of IEC 60870-6), is used for inter-master station communications. (ICS-CERT – Advisory) [DHS 2014].

Electric Infrastructure Security (EIS) Council facilitates national and international collaboration and planning to protect our society's critical utilities against uniquely severe Black Sky Hazards. Our programming and special projects help utilities and their partners develop and implement cost-effective, consensus-based protection measures by hosting frameworks for sustained coordination, planning, and best practice development [EIS Council 2017].

Federal Energy Regulatory Commission (FERC) is an independent agency that regulates the interstate transmission of electricity, natural gas, and oil. FERC also reviews proposals to build liquefied natural gas (LNG) terminals and interstate natural gas pipelines as well as licensing hydropower projects [FERC 2016].

Federal Financial Institutions Examination Council (FFIEC) Cyber security assessment. The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB) and to make recommendations to promote uniformity in the supervision of financial institutions. In 2006, the State Liaison Committee (SLC) was added to the council as a voting member. The SLC includes representatives from the Conference of State Bank Supervisors (CSBS), the American Council of State Savings Supervisors (ACSSS), and the National Association of State Credit Union Supervisors (NASCUS) [FFIEC 2017].

Governance refers to "all processes of governing, whether undertaken by a government, market, or network, whether over a family, tribe, formal or informal organization or territory and whether through laws, norms, power or language." A regulatory agency (also regulatory authority, regulatory body, or regulator) is a public authority or government agency responsible for exercising autonomous authority over some area of human activity in a regulatory or supervisory capacity [Wikipedia 2017].

Information Technology (IT) managed by the CIOs and IT departments, is the application of computers to process, transmit, and store data, typically in a business or enterprise environment [Hayden 2015].

Independent System Operator (ISOs)/Regional Transmission Operations (RTOs) match power generation instantaneously with demand to keep the lights on. ISO and RTO support the latest advancements in smart grid technologies, improving the resiliency and reliability of the grid, making energy transmission more efficient, smarter, and cost effective [ISO /RTO Council 2015].

Incident Command Structure (ICS) is a FEMA management system "designed to enable effective and efficient domestic incident management by integrating a combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure. ICS is normally structured to facilitate activities in five [sic] major functional areas: command, operations, planning, logistics, intelligence and investigations, and finance and administration. It is a fundamental form of management, with the purpose of enabling incident managers to identify the key concerns associated with the incident—often under urgent conditions—without sacrificing attention to any component of the command system" [FEMA 2015].

Industrial Control Systems (ICS) include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) that are often found in the industrial control sectors. ICS are typically used in industries such as electric, water and wastewater, oil and natural

gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods) [NIST 2015].

ICS-CERT works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures [US CERT 2017].

Lineman are also known as line installers and repairers. Line workers repair electric power systems and telecommunication cables, including fiber optics. Line workers encounter serious hazards on the job, including working with high-voltage electricity, often at great heights. The work also can be physically demanding [BLS 2017].

Live-Fire-Exercise (LFX) consists of an on-range network virtual range environment. Network defenders (blue team) are responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers. The opposing force (OPFOR-re team) generally mounts a hostile attack against blue team networks. The LFX objective is to improve enterprise information assurance (cybersecurity) or incident response to enable cyber resiliency by demonstrating the impacts of successful attacks and by demonstrating what works for defenders in an operational environment. A known example is a Cyber Defense Exercise (CDX) that requires a team-oriented approach. There are friendly forces (Blue), hostile forces (Red), technical infrastructure (Green), and game management (White). The Red Team and Blue Teams are the CDX combatants. The Green Team (GT) and White Team (WT) are non-combatants; RT attacks against either in most CDXs are strictly prohibited [Geers 2010].

NC4 is an owned subsidiary, the ESP Group, that exists to deliver safety and security solutions that revolutionize how government and businesses collect, manage, share and disseminate information to reduce cyber threats, fight crime, mitigate risks, manage incidents, and securely communicate and collaborate with one another [NC4 2017].

National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the federal government, intelligence community, and law enforcement. It serves as a central location where a diverse set of partners involved in cybersecurity and communications protection coordinate and synchronize their efforts. NCCIC's partners include other government agencies, the private sector, and international entities. Working closely with its partners, NCCIC analyzes cybersecurity and communications information, shares timely and actionable information, and coordinates response, mitigation and recovery efforts [DHS 2017a].

National Initiative for Cybersecurity Education (NICE). The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST), is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce develop-

ment. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our nation secure [NIST 2017b].

National Initiative for Cybersecurity Education Framework (NCWF) is a national resource that categorizes and describes cybersecurity work. It provides employers, employees, educators, students, and training providers with a common language to define cybersecurity work as well as a common set of tasks and skills required to perform cybersecurity work. Through the process of identifying the cybersecurity workforce and using a standard set of terms, it works to educate, recruit, train, develop, and retain a highly qualified workforce [NIST 2017a].

National Institute of Standards and Technology's (NIST) Framework, also referred to as NIST Cyber Security Framework (CSF), focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles [NIST 2017a].

North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability and security of the bulk power system in North America. NERC develops and enforces reliability standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the bulk power system, which serves more than 334 million people [NERC 2016].

NERC Critical Infrastructure Protection (CIP) Standards are mandatory reliability standards that include CIP standards 001 through 009, which address the security of cyber assets essential to the reliable operation of the electric grid. To date, these standards (and those promulgated by the Nuclear Regulatory Commission) are the only mandatory cybersecurity standards in place across the critical infrastructures of the United States. Subject to FERC oversight, NERC and its Regional Entity partners enforce these standards, which are developed with substantial input from industry and approved by FERC, to accomplish NERC's mission of ensuring the security and reliability of the electric grid. There are nine mandatory CIP standards [NERC 2016].

Nuclear Regulatory Commission (NRC) Regulations - United States NRC- Title 10, Code of Federal Regulation requirements binding on all persons and organizations who receive a license from the NRC to use nuclear materials or operate nuclear facilities [NRC 2017].

Operational Technology (OT) consists of hardware and software systems that monitor and control physical equipment and processes, often found in industries that manage critical infrastructure, such as water, oil and gas, energy, and utilities, but also in automated manufacturing, pharmaceutical processing, and defense networks [Hayden 2015].

Protected Critical Infrastructure Information (PCII) Program enhances voluntary information sharing between infrastructure owners and operators and the government. The Department of Homeland Security (DHS) and other federal, state, tribal, and local analysts use PCII to: (1) Analyze and secure critical infrastructure and protected systems. (2) Identify vulnerabilities and develop risk assessments. (3) Enhance recovery preparedness measures [DHS 2017b].

Regional Resiliency Assessment Program (RRAP) is a cooperative assessment of specific critical infrastructure within a designated geographic area and a regional analysis of the surrounding infrastructure. The RRAP is led by the Department of Homeland Security and addresses a range of hazards that could have regionally and nationally significant consequences. Each year, the department selects voluntary and non-regulatory RRAP projects with input and guidance from federal and state partners [DHS 2017g].

Resilience Presidential Directive-21 defines resilience as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attack, accidents, or naturally occurring threats or incidents. Examples of resilience measures include (1) developing a business continuity plan, (2) having a generator for back-up power, (3) using building materials with increased durability [DHS 2017h].

Stafford Act was signed into law November 23, 1988 and amended the Disaster Relief Act of 1974, PL 93-288. This act constitutes the statutory authority for most federal disaster response activities, especially as they pertain to FEMA and FEMA programs [FEMA 2017a].

Secure Power Systems Cybersecurity Practitioners (SPSP) - DOE Workforce study Purpose: Identify key job skills, education, and certification(s) needed for hiring or retraining Power Systems Cybersecurity (SPSP) practitioners [O'Neil 2015].

Sarbanes-Oxley (SOX) Act of 2002 (often shortened to SOX) is legislation passed by the U.S. Congress to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise, as well as improve the accuracy of corporate disclosures. The legislation came into force in 2002 and introduced major changes to the regulation of financial practice and corporate governance. Named after U.S. Sen. Paul Sarbanes and U.S. Rep. Michael Oxley, who were its main architects, it also set a number of deadlines for compliance and is arranged into 11 titles [Addison-Hewitt Associates 2006].

Supervisory Control and Data Acquisition (SCADA). The major function of SCADA is for acquiring data from remote devices such as valves, pumps, transmitters, and so on and for providing overall control remotely from a SCADA Host software platform. This function provides process control locally so that these devices turn on and off at the right time, supporting control strategy and a remote method of capturing data and events (alarms) for monitoring these processes. SCADA Host platforms also provide functions for graphical displays, alarms, trending, and historical storage of data [Higgins 2013].

Threat and Hazard Identification and Risk Assessment (THIRA) is a four-step common risk assessment process that helps the whole community—including individuals, businesses, faith-based organizations, nonprofit groups, schools and academia, and all levels of government—understand its risks and estimate capability requirements. The THIRA process helps communities

map their risks to the core capabilities, enabling them to determine whole-community, informed, desired outcomes, capability targets, and resources required to achieve their capability targets. The outputs of this process inform a variety of emergency management efforts, including emergency operations planning, mutual aid agreements, and hazard mitigation planning. Ultimately, the THIRA process helps communities answer the following questions:

What do we need to prepare for? What shareable resources are required in order to be prepared? What actions could be employed to avoid, divert, lessen, or eliminate a threat or hazard? [FEMA 2015].

Appendix B Attendance List

Below is the list of those who attended that CMAW. The list includes presenters and participants.

COL Dan Bennett	Army Cyber Institute
CW3 Judy Esquibel	Army Cyber Institute
Ms. Irina Garrido de Stanton	Army Cyber Institute
LTG (R) Rhett Hernandez	Army Cyber Institute
LTC Dan Huynh	Army Cyber Institute
LTC Brett Lindberg	Army Cyber Institute
Dr. Fernando Maymi	Army Cyber Institute
Mr. Brendan Fitzpatrick	CMU-CERT SEI
Mr. Seth Swinton	CMU-CERT SEI
Ms. Lisa Young	CMU-CERT SEI
Mr. Tony Vitello	Citigroup
Ms. Cheryl Maletich	Commonwealth Edison
Ms. Kimberly Smith	Commonwealth Edison
Mr. John Everett	DARPA
Mr. Tim Tkacz	DARPA SETA
Mr. Jim Fama	Edison Electric Institute
Mr. Kelly Cullinane	EIS Council
Mr. Jonathon Monken	EIS Council
Mr. John Organek	EIS Council
Ms. Samara Moore	Exelon
Ms. Laura Ritter	Exelon
Mr. Wayne Austad	Idaho National Laboratories
Mr. Andy Bochman	Idaho National Laboratories
Mr. Carl Kutsche	Idaho National Laboratories
Mr. Tim Yardley	Information Trust Institute, University of Illinois
Mr. Mark Bristow	NCCIC/ICS-CERT
Mr. Javier Fernandez	NextEra Energy
Mr. Bill Lawrence	North American Electric Reliability Corporation (NERC)
Mr. Daniel Holt-Gosselin	NUARI, Norwich University
Mr. Andrew Peterson	NUARI, Norwich University
Mr. Tom O'Brien	PJM Interconnection
Mr. Nick Gaubinger	PowerAdvocate
Mr. Mark McVay	PowerAdvocate
Mr. Lee Rossey	Sim Space Corporation
CPT Robert Morse	USCYBERCOM-CNMF

Appendix C Responses Corresponding to Research Questions

Below are participants' responses to questions discussed in Section 2. All responses are presented in their original state, as submitted, and without editing.

What cyber interdependencies do we need to consider?

There were 40 responses received generally themed on vulnerabilities and cross-sector impacts and focused on telecommunication/communications.

1. Private industry providing power/water to military bases of private industry comes under cyber-attack **who responds**?
2. Has anyone **prioritized** who gets what when it hits the fan?
3. **Supply chain** vulnerabilities for "weakest link" partners on networks
4. **Gas, water, telecommunications, electricity**
5. **Government:** local, state, federal
6. Generation, distribution, transmission, LSE's
7. **Regulators**
8. **Links** between business systems and operational control systems
9. Fuel supply to power generators (particularly gas with no storage)
10. Distributed energy resources (DER) dependency on baseload
11. Power to **nuclear** plants to recovery/blackstart
12. **Communication** dependencies on situational awareness and first responders (i.e., both use LTE/Cell)
13. Areas: **governance**, organizational, process, technical
14. Goals: Eliminate **impedance** mismatch!
15. Cyber-physical
16. **Cross-sector** impacts: financial, dams, pipelines, fuels, water and wastewater
17. **Vendor** support/expertise
18. **Communication** capabilities
19. Cyber-Physical
20. NW/**telecommunication** and cyber security
21. **Intelligence** operations
22. Electricity and **telecommunications**
23. Can't share if in heat of the battle, if **communications** (email, VOIP, cell) are down
24. Satellite phones are often a back-up
25. Many of the **backup or redundant** systems may rely on the same underlying technology (single-point-of failure)
26. **Backup systems** may get overloaded if too many users affected.
27. **Telecommunications** – Emergency (and steady state) response depends on email and phones
28. **Legal** aspects
29. **Policy** aspects
30. **Communications**
31. **Transportation**
32. **Personnel**/Staffing
33. Relationship with Critical Suppliers: **Back-up**, Security for **software** that touches the asset owner, **Vendor** with access to critical **equipment** (during overhaul), **suppliers**
34. **Trust**

35. **Power** underlies everything in our society, so I think of the grid as a vector by which an adversary achieves affects in other sectors. That interdependency is seldom discussed in the context of exercises
36. **I.T. Systems** – **Comms lose** access to procedure/processes
37. ICS/SCADA Architecture similarities **between systems** that can be exploited/leveraged
38. **Security** (Physical) Monitoring
39. Building Management Systems (environmental, etc.)
40. Active Directory? DNS?

Which cyber exercises has your organization participated in?

There were 29 responses received; responders generally participated in strategic and/or regional-level exercises. There was emphasis placed on the need to leverage exercises to produce meaningful outcomes and to take advantage of an opportunity to experiment.

1. Quantum Dawn I, II, III
2. DECIDE-FS Exercise
3. DHS National exercises for institutions of higher education
4. Grid Ex
5. Cyber Guard
6. New York State Cyber Ex
7. Cyber Storm
8. FEMA NLE (National Level Exercise)
9. Internal Tabletop
10. Grid Ex
11. Internal only – Emergency Preparedness focused within Exelon.
12. Grid Ex I, II, III
13. PJM specific to go exercises
14. PJM internal exercises
15. Red/Blue Teaming
16. Quarterly resiliency drills and recovery
17. BCP recovery drills and plans
18. Internal IT, Security OPS Combined Exercise
19. Grid Ex, Cyber Knight, Cyber Guard
20. Would like to develop – Future DARPA exercises that cross industry / DoD
21. CNMF – Cyber Flag, Cyber Guard, Cyber Knight and others when requested such as Pacific Sentry
22. Participate in Cyber Guard – Policy
23. Cyber Guard – hands on
24. DHS sponsored (NLE) Cyber Storm and Hamilton Series
25. NYC OEM Cyber
26. Quantum Dawn FS-exercise
27. Internal tabletops / wargames
28. Cyber Guard
29. Industry

Rules of Engagement for Operational Technology (OT) and Information Technology (IT)

There were 17 responses received themes consisted of situational awareness, thresholds, triggers, anomalies, monitoring systems, drawing the lines between IT and OT, defining the components and having understanding.

1. Need **situational awareness from an IT** perspective of what is going on from an OT perspective whether by change analysis manually or implementing via machine learning.
2. **Physical security** concerns, outages or cyber may effect visibility of network and infra-structure monitoring.
3. Thresholds and triggers for crosstalk during: daily operations, elevated threat, operational anomaly, crisis response, recovery
4. **Operations monitoring** and security monitoring needs to be fused … center
5. Operations monitoring (local and functional context) needs to be core lead/house in order when external IT/security help brought in.
6. Define the "pre…" for OT/critical functions for outside help, analogy: malware forensics: a lot of outside support; if can package context and deliver
7. Governance: both report up to … security exec.
8. Ideally cyber and physical security should also report to one exec.
9. A lot of violation in … others domains
10. Difference between operations problem and insider/outsider sabotage
11. Decision support for risk and realized ….
12. **Training, cross training**, see something say something
13. Pre-identify what are given lanes of IT and OT?
14. Scope of what is IT and OT? What are the boundaries?
15. **Have engineers attend this type of workshop.**
16. OT Forum internally using the language that is meaningful to the specific group.
17. What do the operators need to know about cyber?

What are the legal or regulatory frameworks to be considered?

There were 32 responses. They generally themed around DSCA, Tile 10 vs 32, NIST Framework, information sharing and waivers/compliance/certifications.

1. What gives one the right to be in an information system?
2. Enable utilities to recover most/all their investment in cyber prevention, will likely re-quire some **FERC** mandates
3. Defense Production Act, Stafford Act (not set up for funding private corporations) **EPA waivers**
4. They would need to know **processes or procedure** for Cyber Security Response and probably be notified in event of an attack
5. **NERC CIP Standards**, ES-C2M2, **NIST Framework**, "Top 20" SANS best practices in cyber
6. Immediate response **authority** (IRA) Title 10 versus Title 32
7. **Defense Support to Civil Authority**
8. Security clearance Non-disclosure, **proprietary information, indemnification**
9. Who can I let into my system? NERC/CIP compliance issues?
10. **Non-disclosure agreements**
11. **Federal Anti-Trust Act** – Relating to information sharing
12. Anti-Trust

13. All things that could cause damage to brand/stakeholder impact
14. Safety consideration foremost
15. NERC CIF requirements, NERC requirements, NRC requirements (as applicable)
16. Customer data privacy
17. CNMF – DSCA, currently no cyber DSCA exists, CNMF has forces capable to assist but be invited
18. Non-Disclosure Agreements
19. **The Stafford Act** – gives FEMA authority to coordinate all government disaster recovery activities
20. **State** Anti-Trust Acts as it relates to information sharing
21. Title 32 National Guard – what cyber groups, what functions, who gets called up?
22. Safety Regulations on physical function protection systems Cyber person on …relay, OSHA, NEC
23. Nuclear Power Plan – **NRC Regulations**/background
24. **Spare transformer program at EEI**
25. **Step connect program** at EEI
26. Clear separation between regulatory and operational standards (non – **attribution**)
27. Similar to existing mot considerations
28. NERC C.P exceptional circumstances
29. Does not matter but pick one! Many options!
30. **Breach notification** to regulators
31. **Compromise notification** to regulators
32. **Growing regulator requiring cyber based – exercises**
33. **Federal Financial Institutions Exam Council (FFIEC) Cyber security assessment**
34. **NIST CSF** (aka: NIST Framework)
35. **ES-C2M2**
36. **PCII**/NERC CIP
37. **CISA**

What skillsets are required (IT/OT)?

There were 72 responses received. Themes focused on workforce and talent management in regards to certifications; the needed work roles (commonly seen were forensic, malware, cybersecurity and intrusion analysts); personnel needed to understand the processes (e.g., baselines); understanding equipment, compliance and legal frameworks.

1. Communications Network Engineers
2. Look at Department of Energy SPSP & NICE Competencies
3. Incident Response and Digital Forensics Training (chain of custody, evidence retrieval)
4. Cyber Threat Analyst and Documentation
5. CEH Offensive – Cyber Hunters
6. Malware Analysts
7. GIAC, GICSP
8. Telecommunications Engineer
9. Forensics skills
10. Network Engineer
11. SCADA/ISSP/DNP
12. Database expert on these systems
13. Tconsmission Network Analysis Engineer
14. Operating System Expert
15. Protective Systems Engineers, OT/PLC Configuration engineers
16. ICS specific forensics

17. Consolidated database of skills – taxonomy that sufficiently differentiates important skills – e.g. generator connection electrician,
18. Forensics
19. Data log analysts
20. Net flow Analysts
21. Intrusion Analysts
22. White Hat Hackers/Cyber battle skills
23. Operating System hardening Skills
24. Event Logging Analysis
25. Malware/Anomaly Hunting
26. Protocol Analysis
27. Analytical Skills
28. Forensics
29. How to understand and find when penetration occurs in computer system or attempts are made
30. Forensics (or at least how to isolate/archive systems under suspected attack)
31. SCADA Experts
32. I.T. Network People
33. Engineer Designers
34. Forensics
35. Data Analysis, Threat Analysis
36. Red Teamers/Assessors/Pen Testers
37. Reverse Engineers
38. Malware Analysis
39. Backup, image capture
40. System analysts
41. CISCO
42. Cyber Forensics Team
43. Cyber Risk Analysts Team
44. Forensics
45. Sensor Management
46. IT Skills
47. Understanding Safety e.g. look out tag out
48. Crisis Communications
49. Certified BCP – continuity of business
50. Address SPARES requirements (often overlooked) (back-up equipment, step)
51. Vendor Management
52. Command/control expert that can facilitate listen, and move to specific actions
53. Scribe who can take in multiple inputs and track timelines, actions, new inputs and communicate
54. System Integrators
55. Reliability Coordination on restoration
56. Cyber Security
57. NERC CIP
58. SCADA System operations
59. Soft skills to bridge engagement between IT/OT
60. Baselining Skills
61. Ability to run/understand the system in both automated and manual context
62. Lessons from Ukraine: Running Manual Operations
63. Continuing Education
64. Techniques, Tactics and Procedures of Adversaries
65. Swapping a hardware, preserving the old and replacing with a known good one

66. Skill sets should be grouped into buckets tied to a cyber incident management structure: Identify, Protect, Detect, Respond, Recover
67. Phone Experts
68. Fiber Experts
69. Facility Experts
70. Leadership
71. Identify which skill sets can/should be done by internal assets vs external assistance

What is your understanding of Cyber Mission Forces (CMF) and how can they help?

There were 26 responses received. There was a general understanding that comprehension of the CMF is either limited or unknown. Participants were curious of the capability and how the CMF could help or made suggestions. Lastly, participants wanted to understand how CMF fits into the National Guard.

1. No prior knowledge of Cyber Mission Force
2. Can the cyber mission force – perform vulnerability assessment for organizations - threat info relevant to industry - Provide training and procedures to counter threats.
3. Need way to assess competency or have confidence they won't do more harm on network than organic team.
4. How to know if their info or capabilities are any good or relevant.
5. Have not heard of Cyber Mission Force
6. Determine gaps in system or process prior to event
7. DoD/Army Cyber should have best working knowledge of advanced persistent threats (techniques, tactics, procedures, signatures, etc.)
8. What are the differences with the National Guard capabilities? There are several utilities that have established relationships with National Guard capabilities.
9. One stop shop for what is available, how to partner
10. Use CMF/CPT to prevent cyber restrike attacks while in critical recovery
11. Fuse intelligence from CST against consequence – driven cyber …engineering teardown of critical vulnerability that baseline threat actor capabilities (CCE) proactive intelligence exchange (prioritize and context for information sharing; embedded CNMF/CPT and ICS forces NCCIC/ICS-CERT
12. Publish in one place who and how to engage sector coordinators
13. Improve methods for detection – we must know when we are being attacked, however subtle
14. I don't have much understanding of Cyber Mission Force – How could they help? Boots on the ground, threat intelligence, fill skills gaps, forensics, strategy for mitigation of threat, training, timely support and assistance (this should be pre-planned)
15. How do we get a broad view of what's available in the community from a broader perspective?
16. Are they developing OT support capability?
17. Can we use CRADAs to facilitate government (Army) industry collaborations? Cooperative research and development agreements.
18. Utility legal folks will want to know how data captured in analysis will be safeguarded or preferably destroyed.
19. Limited knowledge capability
20. As of now would say would 0 be invited to touch systems
21. Also any agreements ahead of time (non-disclosure, privacy, report limitations, etc) that would be needed.

22. How do “helpers” get paid? Asset owner, US government, state government dependency on title activity.
23. What is the criteria to use for the cyber equivalent of NRE?
24. What capacity exists to provide direct assistance to private sector for cyber response and recovery IT, OT, ICS/SCADA, how much capacity?
25. Do not know much about it, want to know more.
26. Limited understanding of cyber mission force; how do they differ from ICS-CERT, FBI; value proposition for cyber mission force, US industry service

Pre-incident preparation

There were 106 responses received. There were five common themes, develop – establish partnerships; resiliency – the processes to do so, techniques, tactics and frameworks; exercising – mentioned as a critical component; systems – frameworks configurations (gold disks); focusing on left of boom.

1. Do you know if the data is being manipulated?
2. Do you have sensors in place
3. Do you what good is
4. Do you have clean backups
5. How quickly can you get to the backups
6. Do the backups assume power or some type of risk assessment tool / framework
7. Pre – incident Preparation considerations
8. Internal documentations
9. Internal procedures and processes
10. Communications plan (internal and external)
11. Internal protocol for requesting MA
12. Training on response / repair activities
13. Training needed for MA personnel, specific to the entity
14. Determine whether systems access is needed
15. Non-disclosure agreements
16. Prioritized ICS inventory including: network diagrams, configuration details
17. Build resiliency into your systems, processes and facilities
18. Organization details
19. Contact information
20. With back-up, secondary communications methods ***sounds like Continuity of Operations (COOP) or Continuity Business Plans***
21. Establish strong partnerships and cont…. structures to prepare for various scenarios
22. Process with process for adaptation
23. Restoration Strategy/Plans
24. What infrastructure is at risk for attack (SCADA, Transmission etc.) ***vulnerabilities, attack vectors named are obvious systems***
25. Where are these components in your system?
26. How do operators realize an event is not “normal” but cyber-attack
27. What do I communicate to customers
28. How do I communicate to customers when real time systems are severed from customer communication systems?
29. Identify internal “trigger points” for activating Cyber Capabilities (internally and externally)
30. Delineate tasks for internal vs external personal for response and recovery operations for IT/OT
31. A documented and battle – tested incident response plan

32. Who do I call internally?
33. What other security actions get triggered when cyber event is suspected?
34. Establish internal Cyber Incident Management Process
35. Drill, practice and prepare for scenarios through cross-functional exercises.
36. Legal frameworks access to systems, mutual aid
37. Internal plans/procedures: how communicate internally, who are the players (how do you engage them? What is their role?) Who may you need externally (vendor support, expertise, retainer, other (fly away teams) regulated aspects, reporting; public affairs protocols – internal and external (government, media, customers, etc) skill set identification – needed for cross-training; legal impacts – non-disclosure agreements, prioritization, retainers.
38. Adaptation Strategy/Plans
39. Critical Elements of Information
40. Development of techniques for mission/incident
41. Prepare / review threat/technique tactics manual
42. Deploy sensors (tune existing)
43. Create a baseline (to compare to manufacture baseline)
44. Analyze baseline and look for Delta
45. Phone numbers of all first responders that can provide assistance: DoD, DHS, FBI, etc.
46. Have a strong process with clear roles and responsibilities
47. Incident Response Plans
48. Pre-established communication templates approved
49. Playbook and Plan Exercises + Drills
50. Executive Management Awareness – Exercises
51. Delegation of Authority models socialized and tested
52. Defined escalation criteria
53. Network Diagrams
54. Gold Disks for all equipment
55. Know most important assets to delivery critical power and their digital dependency (what is the most important to protect/recovery)
56. Which assets do not have manual/Labor options currently?
57. Who is the vendor supply/integrator with knowledge of system configuration (and their alternatives)
58. Parts and recovery that require your folks
59. Baseline your systems so know what normal looks like
60. Asset Identification
61. Configuration management (gold disks)
62. Know what your key assets are, how they are linked, what dependencies do they have, what backups (links, data, vendors) are available, know who the experts are to resolve.
63. Keep IT and OT systems patched, create and maintain gold disks of all required firmware, configuration files, circuit patches, operating systems etc to restore system from scratch
64. Keep gold disks offline, not accessible to hackers
65. Keep it current (gold disks) and available to employees who may need it
66. Use it in exercises, find out how hard it would be to restore from scratch
67. Turn on logging on IT and OT systems
68. Archive logs offline best accessible in an emergency
69. Analyze logs to determine what normal operations looks like over the course of a year, to enable more effective identification of anomalies
70. POV: a utility: map of internal vs external capabilities; strong map/network diagrams, understanding the technical landscape
71. Internal capabilities: where are they resident, how redundant are they, how readily can they be accessed

72. External capabilities who provides these and skills/abilities/pieces of equipment how deep is that base of supply? How quickly can these recoveries be accessed?
73. Secure communications channel
74. Spare clean equipment and capability to transport IT
75. Legal Liaison
76. Forensics Experts
77. Cyber Mutual Assistance Playbook
78. A pre-established communications plan and options is important (out of band communications, etc.)
79. Human Resources Policies (overtime, etc.)
80. First person knowledge and interfacing between people from both the same and different silos
81. Training and "en-actment" of the plans so they are exercised in practice not just written and shelved
82. External entities (with depth) to call on existing non-disclosure agreements, contracts, etc. In place to enable quick action.
83. Internal assets and configuration auditing (keeping repositories of both)
84. Well defined processes and call tree for escalation with pre-defined criteria for escalation
85. Detailed and current topologies and infrastructure details
86. Engage with and visit your state emergency operation centers, and or fusion centers. Some are co-located on military bases and are more difficult to access. These may have classified briefing capabilities for use during incidents.
87. Know you equipment: what is it, where is it, where is it in respect to anything else? What skills are needed to control and manage it? Who else has it?
88. Standardized request format that includes specific skills
89. Standardized in-brief (and read-ahead) for external helpers
90. Access credentials for devices (username and passwords)
91. Utilities: Take advantage of electricity ISAC membership: EISAC portal, incident sharing hotline, email or user groups, immediate notifications and daily/weekly/monthly/annual reports; for cyber (IT/OT) and physical security passwords
92. Compliance Risk Free!
93. Identify critical skills sets certifications and capability for internal IT and OT systems
94. Have effective up-to-date, and accurate picture of your systems and the configurations
95. Develop and practice incident response plans
96. What will organizations look like for the mutual aid team
97. Each Electric company would need a standardized book/manual for what their systems look like (network topologies, etc)
98. Identify pool of cyber experts that can be deployed anywhere (based on pre-defined qualifications)
100. Check lists of steps to take once incident occurs – including contacts to call and numbers
101. Know procedure (once written) throughout
102. Once the above steps are completed exercise it, practice, practice, practice
103. Suppliers – who are the suppliers providing critical assets, can they provide backup inventory/service when needed for attack recover; can you be certain they won't introduce another problem?
104. Certify that components you purchase are protected. How about tier 2 vendors do they provide a risk?
105. Contract up local law enforcement to educate them on critical assets in the region
106. Have an exercises + socialized playbook/SOP/etc

What are the critical assets?

There were 58 responses received. There were four common themes: identifying communications systems and additional capability; processes necessary to enable incident response; understanding of current frameworks of incident handling (legal aspect); and the importance of knowing the people or organizations involved.

1. End-to-end analysis with operational outcome impact
2. Any systems, people, tools, data, or process that required to keep the lights on.
3. Real time systems
4. Control rooms – primary and back-up
5. Laptops
6. Substations – critical
7. Data Centers where servers that control real-time systems reside
8. Communications systems (fiber to subs)
9. Each sector defines – what component why it is important how hard to replace/restore/time/cost/other)
10. Logs (data backup), SCADA, EMS, forensic capability, netflow expertise, firewall expertise, malware expertise, IS landing capability, secure communications systems
11. STEM systems, log systems, packet tapping, capture systems for incident response
12. Communication systems: phone, chat, email, etc (trust and response)
13. Contracts/legal and the external companies to respond on cyber
14. Downstream data, systems, starts that a critical function and must have "x" minutes/hours into an event to sustain the mission of keeping the lights on.
15. Build a cyber/physical asset interdependence crosswalk for risk assessment and prioritization
16. Full and current understanding of all internet connected systems/devices with VPN firewall details
17. What Cyber assets are considered so critical that they are kept running 24/7, perhaps never patched or taken offline (if any)? What cyber assets would never be considered for inclusion in an exercise that would subject them to unusual stress? Is the practice of keeping these assets running by shielding then from any form of stock making them even more fragile?
18. SCADA systems, EMS (Emergency Management Systems), Outage Management Systems (OMS), control centers, CUR
19. Communications or information
20. Are you doing passive/active asset identification, know what is talking on your network
21. Where there is a "wire" (or wireless) there is a way even if it's serial (where we are likely not monitoring well)
22. People
23. Any NERC designated asset plus many non NERC assets in distribution
24. Security Operations Center
25. Cyber Security Fusion Centers – fusing information from cyber intelligence, security operations, and investigative
26. 3rd party (vendor) integration (monitoring)
27. Data Center
28. First cut at personnel asset "typing" for capability assessment and mission assignment.
29. Physical security systems for access into plants
30. Sarbanes Oxley (severs, etc.)
31. Have you done a **dependency mapping**
32. Do you have back-ups, alternate vendors, alternate SW loads, clean images if an adversary has manipulated the SW in place or at the vendor.
33. What IT assets do they rely on

34. Any vendor who can access critical cyber assets – employee computer assets
35. Emergency Restart Equipment
36. SAAS Software connected to operational assets
37. Software supporting Cyber design collaboration with vendors
38. **Sensor strategy**; response forces and command and control of incident, intelligence, forensics, and analysis, mitigation tools and techniques
39. Substations
40. SCADA
41. Facilities
42. Network I.T.
43. Communications, phones and radios
44. Computers
45. Water pumping stations
46. **Nuclear plants**
47. **Hospitals**
48. Transportation Airlines
49. Supply chain/payroll systems
50. Environmental control systems for data centers (AC,etc)
51. People – qualified …. And cross-over skill sets (DTTO (NUARI)
52. Processes – Incident response plans, continuity of operation plans
53. Protective equipment (i.e. relays, physical grid operations)
54. Engineers with configuration knowledge of safety, protective systems
55. Reliability coordinators that understand failure/recovery modes.
56. Energy Management Systems, situational awareness
57. See NERC Critical infrastructure protection (CIP) version 5. These standards require electric entities to identify critical cyber assets on a high/medium/low impact scale. They go into effect 01JUL16
58. Establish industry standards for physical Cyber Asset “Tiers” i.e. control centers vs data centers vs data linkages vs. sensor networks.

References

URLs are valid as of the publication date of this document.

[Addison-Hewitt Associates 2006]
A Guide to the Sarbanes-Oxley Act. *Addison-Hewitt Associates, B2B Consultancy*. October 2, 2017 [accessed]. http://www.soxlaw.com/

[ARL 2017]
Cooperative R&D Agreements. U.S. Army Research Lab. September 29, 2017 [accessed]. https://www.arl.army.mil/www/default.cfm?page=14

[BLS 2017]
Bureau of Labor Statistics. Line Installers and Repairers. *Occupational Outlook Handbook, 2016-17 Edition. United States Department of Labor.* October 2, 2017 [accessed]. http://www.bls.gov/ooh/installation-maintenance-and-repair/line-installers-and-repairers.htm

[DHS 2014]
DNP3 Implementation Vulnerability (Update B). Advisory (ICSA-13-291-01B). ICS-CERT. *U.S. Department of Homeland Security*. October 2, 2017 [accessed]. https://ics-cert.us-cert.gov/advisories/ICSA-13-291-01B

[DHS 2016c]
Information Sharing Specifications on Cybersecurity. *U.S. Department of Homeland Security*. September 29, 2017 [accessed]. https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

[DHS 2017a]
National Cybersecurity and Communications Integration Center. Department of Homeland Security. October 3, 2017 [accessed]. https://www.dhs.gov/national-cybersecurity-and-communications-integration-center

[DHS 2017b]
Critical Infrastructure Cyber Community C³ Voluntary Program. *U.S Dept. of Homeland Security*. September 29, 2017 [accessed]. https://www.dhs.gov/ccubedvp

[DHS 2017c]
Critical Infrastructure Sectors. *U.S Department of Homeland Security*. September 29, 2017 [accessed]. https://www.dhs.gov/critical-infrastructure-sectors

[DHS 2017d]
Sector Specific Agencies. *U.S. Department of Homeland Security*. September 29, 2017 [accessed].https://www.dhs.gov/sector-specific-agencies

[DHS 2017e]
NICE Cybersecurity Workforce Framework. *National Initiative for Cybersecurity Careers and Studies.* U.S. Department of Homeland Security. September 29, 2017 [accessed]. https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

[DHS 2017f]
Protected Critical Infrastructure Information Program. *Department of Homeland Security*. October 2, 2017 [accessed].
https://www.dhs.gov/protected-critical-infrastructure-information-pcii-program

[DHS 2017g]
Regional Resiliency Assessment Program. *Department of Homeland Security*. October 2, 2017 [accessed]. https://www.dhs.gov/regional-resiliency-assessment-program

[DHS 2017h]
What is Security and Resilience? *Department of Homeland Security*. October 2, 2017 [accessed]. https://www.dhs.gov/what-security-and-resilience

[DoD 2013]
Department of Defense. Chairman of the Joint Chiefs of Staff (CJCS), *Defense Support of Civil Authorities (DSCA).* Joint Publication 3-28. July 31, 2013.
http://www.dtic.mil/doctrine/new_pubs/jp3_28.pdf

[DoD 2014]
'Cyber Flag' Exercise Tests Mission Skills. *U.S Department of Defense.* November 12, 2014.
http://www.defense.gov/News-Article-View/Article/603637

[DoD 2015]
The Department of Defense Cyber Strategy. U.S Department of Defense. April 2015. September 29, 2017 [accessed]. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[DoD 2016a]
Cyber Guard 16 Fact Sheet. U.S. Cyber Command News Release. *U.S. Department of Defense*. September 29, 2017 [accessed]. http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Cyber-Guard-16-FactSheet-FINAL.pdf

[DoD 2016b]
All Cyber Mission Force Teams Achieve Initial Operating Capability From A U.S. Cyber Command News Release October 24, 2016. https://www.defense.gov/News/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability/

[DoD 2016c]
Cyber Shield 2016. Defense Media Activity. *U.S Department of Defense*. September 29, 2017 [accessed]. https://www.dvidshub.net/feature/cybershield2016

[DOE 2017]
Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). Office of Electricity Delivery & Energy Reliability. *U.S. Department of Energy website*. September 29, 2017 [accessed]. http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity

[EC-Council 2017]
Certified Ethical Hacking Certification. EC-Council. http://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ September 29, 2017 [accessed].

[EEI 2016]
Understanding the Electric Power Industry's Response and Restoration Process. *Edison Electric Institute (EEI).* October 2, 2017 [accessed]. http://www.eei.org/issuesandpolicy/electricreliability/mutualassistance/Documents/MA_101FINAL.pdf

[EIS Council 2017]
Electric Infrastructure Security Council. *Electric Infrastructure Security Council.* October 2, 2017 [accessed]. http://www.eiscouncil.com/

[EPRI 2017]
Distributed Energy Resources (DER). *Electric Power Research Institute.* September 29, 2017 [accessed]. http://www2.epri.com/Our-Work/Pages/Distributed-Electricity-Resources.aspx

[FEMA 2015]
Threat and Hazard Identification and Risk Assessment. *Federal Emergency Management Agency.* October 3, 2017 [accessed]. https://www.fema.gov/threat-and-hazard-identification-and-risk-assessment

[FEMA 2017a]
Robert T. Stafford, Disaster Relief and Emergency Assistance Act, as amended, and Related Authorities as of August 2016. *Federal Emergency Management Agency*. October 3, 2017 [accessed]. https://www.fema.gov/media-library/assets/documents/15271

[FEMA 2017b]
Operations-Based Exercises. IS-120.a Training Module, Emergency Management Institute. *Federal Emergency Management Agency.* October 2, 2017 [accessed]. https://emilms.fema.gov/IS120A/m1p14.htm

[FEMA 2017c]
Defense Production Act Authorities. *Federal Emergency Management Agency.* October 2, 2017 [accessed]. https://www.fema.gov/defense-production-act-overview

[FERC 2016]
What FERC Does. *Federal Energy Regulatory Commission.* October 2, 2017 [accessed]. https://www.ferc.gov/about/ferc-does.asp

[FFIEC 2017]
Welcome to the Federal Financial Institutions Examination Council's (FFIEC) Web Site. *Federal Financial Institutions Examination Council.* October 2, 2017 [accessed]. https://www.ffiec.gov/

[FTC 2017]
Anti-Trust Law. *Federal Trade Commission website.* September 29, 2017 [accessed]. https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/antitrust-laws

[Geers 2010]
Geers, K. Live Fire Exercise: Preparing for Cyber War. *Journal of Homeland Security and Emergency Management.* Volume 7. Number 1. Article 74. 2010. https://doi.org/10.2202/1547-7355.1780

[Ghernaouti 2013]
Ghernaouti, Solange. CTF competition exercise. *Cyber Power-Crime, Conflict and Security in Cyberspace.* pg. 193. EPFL Press. ISBN-10: 146657304X. 2013.

[Harp 2017]
Harp, Derek R; Gregory-Brown, Bengt, IT/OT Convergence Bridging the Divide. *Nexdefense.* October 2, 2017 [accessed]. http://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf

[Hayden 2015]
Hayden, Ernie. Information Technology (IT) vs Operations Technology (OT): What the C-Suite Needs to Know. *Hazar Strategy Institute (HASEN).* August 13, 2015. October 3, 2017 [accessed]. https://www.hazar.mediaclick.work/en/analysis/information-technology-it-vs-operations-technology-ot-what-the-c-suite-needs-to-know

[Higgins 2013]
Higgins, Kelley Jackson. The SCADA Patch Problem. *Darkreading, InformationWeek.* October 2, 2017 [accessed].
http://www.darkreading.com/vulnerabilities---threats/the-scada-patch-problem/d/d-id/1138979?

[InfraGard 2016]
InfraGard: Partnership for Protection. 2016. October 3, 2017 [accessed]. https://www.infragard.org/

[ISACA 2017]
Certified Information Systems Auditor (CISA). September 29, 2017 [accessed].
http://www.isaca.org/certification/cisa-certified-information-systems-audDNP3itor/pages/default.aspx

[ISO / RTO Council 2015]
About the IRC. *ISO/RTO Council*. October 2, 2017 [accessed]. http://www.isorto.org/About/Role

[Kick 2014]
Kick, Jason. Cyber Exercise Playbook. MITRE Corporation. November 2014. MP140714. Wiesbaden, Germany. October 2, 2017 [accessed]. https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf

[NC4 2017]
NC4 Overview. NC4. October 3, 2017 [accessed]. http://nc4.com/Pages/CompanyOverview.aspx

[NERC 2016]
About NERC. *North American Electric Reliability Corporation.* October 3, 2017 [accessed]. http://www.nerc.com/AboutNERC/Pages/default.aspx

[NIST 2014]
Framework for Improving, Critical Infrastructure Cybersecurity. Version 1.0, National Institute of Standards and Technology. February 12, 2014. October 2, 2017 [accessed]. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[NIST 2015]
National Institute of Standards and Technology. *Guide to Industrial Control Systems (ICS) Security*. NIST Special Publication (SP) 800-82 Revision 2 Final Public Draft. 2-16 and 2-17. pp. 34-35. February 2015. October 2, 2017 [accessed].

[NIST 2017a]
Newhouse, William; Stephanie Keith, Benjamin Scribner, and Greg White. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF). NIST Special Publication 800-181. August 2017. October 3, 2017 [accessed]. https://doi.org/10.6028/NIST.SP.800-181

[NIST 2017b]
National Initiative for Cybersecurity Education (NICE). October 3, 2017 [accessed]. https://www.nist.gov/itl/applied-cybersecurity/nice/about

[Norwich University 2015]
Distributed Environment for Decision-Making Exercise – Financial Sector (DECIDE-FS) Norwich University News - website. November 12, 2017 [accessed]. http://oc.norwich.edu/blog/norwich-universitys-cyber-gaming-software-utilized-in-quantum-dawn-3-cybersecurity-exercise/

[NRC 2017]
NRC Regulations - Title 10, Code of Regulations. U.S. Nuclear Regulatory Commission. October 3, 2017 [accessed]. http://www.nrc.gov/reading-rm/doc-collections/cfr/

[NSA 2016]
Cyber Defense Exercise (CDX). Information Assurance. *The National Security Agency*. September 29, 2017 [accessed]. https://www.iad.gov/iad/programs/cyber-defense-exercise/

[O'Neil 2015]
O'Neil, L. R., F. L. Greitzer, T. J. Conway, A. C. Dalton, D. H. Tobey, and P. K. Pusey. Secure Power Systems Professionals (SPSP) Phase III, Final Report: Recruiting, Selecting, and Developing Secure Power Systems Professionals: Job Profiles. *Pacific Northwest National Laboratory.* Richland, Washington. October 2, 2017 [accessed]. http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-24138.pdf

[Risto 2015]
Risto, Jonathan. Exercising - Not Just for Your Body Anymore. A comparative examination of the types of cyber exercises possible. *SANS Institute InfoSec Reading Room*. January 20, 2015. October 2, 2017 [accessed]. https://www.sans.org/reading-room/whitepapers/training/exercise-body-anymore-35782

[SEI 2017a]
CERT Resilience Management Model (CERT-RMM). CERT, Software Engineering Institute. Carnegie Mellon University. September 29, 2017 [accessed]. http://www.cert.org/resilience/products-services/cert-rmm/cert-rmm-model.cfm

[SEI 2017b]
About Us: the CERT Division. CERT, Software Engineering Institute. Carnegie Mellon University. September 29, 2017 [accessed]. http://www.cert.org/about/

[U of W-M 2012]
What is a Table-Top-Exercise? *University of Wisconsin-Madison Police Department*. May 9, 2012. http://uwpd.wisc.edu/content/uploads/2014/01/What_is_a_tabletop_exercise.pdf

[US CERT 2017]
The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). U.S. CERT. *Department of Homeland Security.* October 3, 2017 [accessed]. https://ics-cert.us-cert.gov/

[Wikipedia 2017]
Governance. Wikipedia. October 2, 2017 [accessed]. https://en.wikipedia.org/wiki/Governance

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	February 2018	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Cyber Mutual Assistance Workshop Report	FA8721-05-C-0003

6. AUTHOR(S)

Jonathon Monken, Fernando Maymi, Dan Bennett, Dan Huynh, Blake Rhoades, Matt Hutchison, Judy Esquibel, Bill Lawrence, Katie Stewart

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2018-SR-007

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

This report describes a Cyber Mutual Assistance Workshop (CMAW), its significance, and its outcomes. The CMAW was intended to explore the interconnectedness of the North American Power Sector and possible sources of aid, should the sector fall victim to a cyber attack. The objective of the CMAW was to enable better understanding of capabilities, not only in the sector's own cyber security workforce, but in possible mutual support from city, state, and federal government entities, and across other sectors' cyber security communities. The Army Cyber Institute, alongside the Electric Infrastructure Security Council and the Software Engineering Institute's CERT Coordination Center, aimed to explore and evoke national conversation on the possibility of mutual cyber assistance in times of duress and the importance to that endeavor of prior understanding and relationships between concerned parties.

14. SUBJECT TERMS	15. NUMBER OF PAGES
resiliency, North American Power Sector, cyber attack	53

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18
298-102